USER'S GUIDE

Release 1.2.0

Cabletron Systems

(603) 332-9400 phone
(603) 337-3075 fax
support@ctron.com

Only qualified personnel should perform installation procedures.

NOTICE

You may post this document on a network server for public use as long as no modifications are made to the document.

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

©Copyright 1997 by Cabletron Systems, Inc. All rights reserved.

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Order Number: 9032432

VIRUS DISCLAIMER

Cabletron Systems has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © July 1997, by Cabletron Systems, Inc. All rights reserved.

TRADEMARKS

CyberSWITCH and SecureFast Virtual Remote Access Manager are trademarks of Cabletron Systems, Inc.

All other product names mentioned in this manual are trademarks or registered trademarks of their respective companies.

COPYRIGHTS

All of the code for this product is copyrighted by Cabletron Systems, Inc.

© Copyright 1991-1997 Cabletron Systems, Inc. All rights reserved. Printed in the United States of America.

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. (“Cabletron”) that sets forth your rights and obligations with respect to the Cabletron software program (the “Program”) contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CONTENTS

Using This Guide 10
- About this Guide 10
- Documentation Set 11
- Guide Conventions 12

System Overview 13
- The SFVRA Connection Manager Network 13
- Unique System Features 14
- Interoperability Overview 15
  - Interoperability Protocols 15
  - Interoperability Devices 16
- Remote ISDN Devices 16
- System Components 17
- Before You Install SFVRA Connection Manager 17
  - System Requirements 17
    - Server PC Requirements 17
    - Client PC Requirements 18
  - Policies for Configuration 18
  - Network Topology 19

System Installation 21
- Installing the SFVRA Connection Manager System 21
  - Installing the MS SQL Server 21
  - Installing the ODBC Drive Pack 3.0 21
  - Installing the SFVRA-CONN Software 24
  - Installing the SFVRA Database 25
  - Installing the NDIS Driver 26
- Installing the Simple Network Management Protocol 26
  - Installing Windows NT SNMP Service 27
  - Configuring the SNMP Service 27
  - Compiling the MIB File 27
- Installing Adobe Acrobat Reader 28

Using the SFVRA-CONN Application 29
- Overview 29
- Starting the SFVRA-CONN Client 29
- SFVRA Service 30
- RIP Service 31
- Proxy ARP Service 31
- Starting and Stopping the SFVRA-CONN Services 32

Configuring Remote Access Switches 33
- Overview 33
- CyberSWITCH Properties 34
  - Configuring Remote Access Switch Properties 35
- Priority Users 36
  - Configuring Priority Users 37
- Pooling 37
  - Configuring Remote Access Switch Pooling 39

Configuring Users 40
Overview 40
Address 41
Configuring User Address 42
Configuring User Categories 42
Protocols 42
IP 43
Configuring the IP Protocol 44
Static Routes 45
Configuring Static Routes 46
IPX 46
IPX Option Background Information 46
Configuring the IPX Protocol 48
IPX Spoofing 49
Watchdog Protocol 49
SPX Protocol 50
Configuring IPX Spoofing 52
Bridging 53
Configuring the Bridging Protocol 55
IP Remote LAN 55
Configuring IP Remote LAN 55
IPX Remote LAN 56
IPX Spoofing on a RLAN Interface 56
Configuring IPX RLAN 57
AppleTalk 58
Configuring the AppleTalk Protocol 59
Restrictions 60
Configuring Restrictions 63
Access 63
Authentication 63
Device Level Authentication on SFVRA-CONN 63
Offnode User Level Authentication with SFVRA-CONN Device Level Authentication 64
Configuring Authentication 68
Grouping Users 68
Configuring Grouping 69
Other 70
Compression 70
Callback 70
Configuring Other Features 72
Telephone 72
Configuring Telephone 75
Usage 76
Viewing and Resetting Call Usage 77

Configuring CyberSWITCH - User Groups 78
Overview 78
CyberSWITCHES 79
Grouping CyberSWITCHES 79
Users 80
Grouping Users 81
View 81
Viewing Groups 82
Creating a New Group 82

Configuring Network Proxies 83
Overview 83
Properties 83
Configuring Routing Properties 84
SFVRA Services 84
Configuring SFVRA Services 85
Network Proxies 86
Configuring Network Proxies 88

Monitoring Connections 89
Overview 89
Current Connections 89
Viewing Current Connections 91
Connect History 92
Viewing Past Connections 93
Connect History Manager 93
Managing the Call and Connect History Tables 95
Problem Log 96
Viewing the Problem Log 98
Problem Log Manager 98
Managing the Problem Log 99
Connection Reports 100
Creating Reports 102
Database Information 103
Viewing Database Information 104

Routine Maintenance 105
Overview 105
Configuration Back Up 105
Upgrading the SFVRA-CONN Software 105
Upgrading the SFVRA Database 107

System Verification 108
Overview 108
Verifying a TCP Connection to SFVRA 108
Verifying the Possibility of a TCP connection 108
Verifying an Existing TCP Connection 108
Verifying that SFVRA-CONN has been Enabled on a CyberSWITCH 109
Verifying Group Assignments 110

Problem Diagnosis 111
Overview 111
TCP Connections 111

System Messages 112
Overview 112
Client Interface Messages 112
Error Messages 112
Warning Messages 117
Informational Messages 117
Interrogative Messages 118
SQL Error Messages 121
Problem Log Messages 121
Failure Messages 121
Reasons for Failure 122

SQL Setup Utility 124
Overview 124
Configuring the SQL Service for SFVRA-CONN 124
Expanding the Size of tempdb 126
Upgrading the SQL Service for SFVRA-CONN 127

Manage Logins 129
Overview 129
Creating Login Accounts for Clients 130

Convert 131
Overview 131
CyberSWITCH Configuration Files 132
Transferring .NEI Files 134
Converting CSX Configuration Files 134
Data Files 134
Converting a Data File 135
Convert System Messages 135
Error Messages 136
Warning Messages 137
Informational Messages 138
Interrogative Messages 138

CSX Monitor 139
Overview 139
Running the CSX Monitor 140

Bridging Network Example 141
Overview 141
Initial Installation Steps 141
Network Topology 142
System Details 143
Resources 143
Lines 143
Bridging 143

Configure the CyberSWITCH 144
Configuring the CyberSWITCH to Interact with SFVRA-CONN 144
Configuring the CyberSWITCH to Interact with Bridge Users 144
Configure the CyberSWITCH - User Grouping 145
Configure the CyberSWITCH on SFVRA-CONN 145
Configure User Records 146
Verify Configurations 151

IP Network Example 152
Overview 152
Initial Installation Steps 152
Network Topology 153
System Details 154
Resources 154
Lines 154
IP Routing 154
Configure the CyberSWITCH 155
Configuring the CyberSWITCH to Interact with SFVRA-CONN 155
Configuring the CyberSWITCH to Interact with IP Users 155
Configure the CyberSWITCH - User Grouping 156
Configure the CyberSWITCH on SFVRA-CONN 156
Configure User Records 157
Configuring IP WAN Users 157
Configuring IP WAN Users with Remote Bridge Devices 161
Configuring an IP WAN User with a PPP Device 163
Configure Network Proxies 166
Verify Configurations 168

IPX Network Example 169
Overview 169
Initial Installation Steps 169
Network Topology 170
System Details 171
Resources 171
Lines 171
IPX Routing 171
Configure the CyberSWITCH 172
Configuring the CyberSWITCH to Interact with SFVRA-CONN 172
Configuring the CyberSWITCH to Interact with IPX Users 172
Configure the CyberSWITCH - User Grouping 173
Configure the CyberSWITCH on SFVRA-CONN 173
Configure User Records 174
Configuring IPX WAN Users 174
Configuring Remote LAN Users 179
Configure Network Proxies 181
Verify Configurations 183

AppleTalk Network Example 184
Overview 184
Initial Installation Steps 184
Network Topology 185

System Details 186
Resources 186
Lines 186
AppleTalk Routing 187
Configure the CyberSWITCH 188
Configuring the CyberSWITCH to Interact with SFVRA-CONN 188
Configuring the CyberSWITCH to Interact with AppleTalk Users 188
Configure the CyberSWITCH - User Grouping 189
Configure the CyberSWITCH on SFVRA-CONN 189
Configure User Records 190
Configure Network Proxies 195
Verify Configurations 197

SQL Database Script Definitions 198
Overview 198
SFVRA Database Tables 198
ACCESS_SERVER 198
ACCESS_SERVER_STATUS 200
CALLING_NUMBERS 200
IP_POOL 201
STATIC_IP_ROUTES 201
PROBLEM_LIST 202
FAILURE_TYPES 202
REASON_STRINGS 202
CALL_HISTORY 203
CONNECT_HISTORY 204
CURRENT_CALL 205
CURRENT_CONNECT 206
USER_ACCESS 207
USER_ACCUM 214
USER_CATEGORIES 214
USER_INFO 215
USER_RESERVED 216
USER_AUTHENTICATIONS 217
USER_CONNECTTYPES 217
USER_LAYER2 217
USER_CALLDIRECTIONS 217
CONN_REPORT_HDR 218
CONN_REPORT_DET 218
ROUTING_PROTOCOLS 218
CURRENT_TIME_EX 218
GROUPS 218
USER_GROUPS 219
SFVRA_SERVER 219
RIP_SERVICE 219
VERSION 220

Getting Assistance 221
Reporting Problems 221
Contacting Cabletron Systems 221

Index 223

USING THIS GUIDE

This guide provides an overview as well as instructions for installing and configuring the SecureFast Virtual Remote Access Connection Manager (SFVRA-CONN or SFVRA Connection Manager). This guide has been written for the network administrator responsible for setting up, configuring, and maintaining SFVRA Connection Manager systems.

ABOUT THIS GUIDE

The *User's Guide* describes the software installation, configuration, and maintenance of SFVRA-CONN. Specifically:

The *System Overview* chapter provides a basic description of the SFVRA Connection Manager network. It includes features specific to the SFVRA-CONN, system requirements, policies for consideration, and a general network topology.

The *System Installation* chapter provides a step-by-step description for configuring the ODBC drivers and installing the SFVRA Connection Manager software. It also discusses the installation and configuration of SNMP on your network.

Using the SFVRA-CONN Application provides instructions for starting the Client application. It also describes SFVRA Connection Manager services and how to start and stop them.

Configuring Remote Access Switches provides instructions for configuring the Remote Access Switches administered by SFVRA Connection Manager. General properties are required for configuration, however Priority Users and IP Pooling may also be configured.

Configuring Users provides instructions for configuring each user that calls into the Remote Access Switches. Features such as user protocols, call restrictions, and authentication are configured here.

Configuring CyberSWITCH - User Groups provides instructions for configuring groups to help you better manage your network. CyberSWITCH systems and users may be grouped to distinguish calling areas, different user protocols, corporate access, or by whatever criteria to determine.

Configuring Network Proxies provides instructions for configuring system wide dynamic routing, and the locations of the SFVRA, RIP, and Proxy ARP Services.

The *Monitoring Connections* chapter provides information on monitoring past and present connections, as well as those that had problems. Also included is a section on creating reports and viewing general database statistics.

Routine Maintenance provides instructions for backing up the database files and for performing SFVRA Connection Manager application and database software upgrades.

System Verification provides a method for verifying your system installation.

Problem Diagnosis includes steps to take if problems occur.

System Messages provides system messages that may be used to troubleshoot if necessary. Each message that is listed provides a definition and a suggested action you can take.

The *SQL Setup Utility* chapter walks you through an application which configures your SQL Server for use with SFVRA Connection Manager.

The *Manage Logins* chapter describes how to use an application which allows you to configure various login accounts for SFVRA Connection Manager.

The *Convert* chapter describes how to use an application that will convert .NEI files from the CyberSWITCH systems or a flat file containing the user name and password into the SFVRA database.

The *Monitor* chapter explains an application which gives you a broad view of current TCP connections and current calls to remote users.

The *Bridging Network Example* provides bridging configuration instructions which may be helpful in configuring a similar network. This example describes a simple network with remote bridge devices.

The *IP Network Example* provides IP configuration instructions which may be helpful in configuring a similar network. This example describes a network with Direct Host PC, an IP user with a remote bridge device, and an IP user with a PPP device.

The *IPX Network Example* provides IPX configuration instructions which may be helpful in configuring a similar network. This example describes a network which supports Remote LAN bridging devices, and a remote IPX router.

The *AppleTalk Network Example* provides AppleTalk configuration instructions which may be helpful in configuring a similar network. This example describes a network which supports two LANs with Macs separated by a WAN.

The *SQL Script Database Definitions* chapter describes every field in the SFVRA database. Advanced SQL users are then able to run SQL queries about any data desired.

Getting Assistance provides information for getting assistance if you run into problems with your system. A FAX form is included. You can copy this form, fill out the information requested, and FAX it to Cabletron Systems, using the provided FAX number.

DOCUMENTATION SET

The *User's Guide*, provides detailed information to install and configure your system. Several examples are provided to aid you in the installation and configuration of the SFVRA Connection Manager and the systems that it administers. It also provides information you can use to keep your SFVRA-CONN running smoothly. The User's Guide introduces several sample networks which provide configuration instructions that you may find helpful in configuring your own similar network.

Context-sensitive help is available for fields within the user interface. To activate context-sensitive help, Windows NT users can use the mouse to select the field in question and press <F1>. Buttons can be selected by using the Tab key.

The *Release Notes* provide release highlights and important information related to this release that you should review before you configure the SFVRA-CONN. The Release Notes are provided in a file that can be accessed under the Help menu of SFVRA Connection Manager's Client interface.

GUIDE CONVENTIONS

The following conventions are used throughout the documentation:

SYSTEM COMMANDS

All commands are italicized, and in a different font than the general text. For example, if you are instructed to enter the path for the location of the NDIS driver, the command would appear as follows:

c:\Program Files\SFVRA-CONN\driver

DOCUMENTATION TITLES

All references to Documentation and Chapter titles will use the same font as normal text, but will be italicized. For example, all references to the chapter Configuring Users will appear as:

Configuring Users

GRAPHICAL INTERFACE BUTTONS, FIELDS AND MENUS

All references to graphical interface buttons, fields and menus will use the same font as normal text, but will be italicized. For example, if you are configuring authentication for a user you will be instructed to:

Select *Authentication* on the *Access* tab.

MONITOR DISPLAYS

Any messages or text that is displayed on your monitor will be portrayed in the documentation in the style shown below:

```
LAN Port <port #> is now in the LISTENING state
WAN Port <port #> is now in the FORWARDING state
LAN Port <port #> is now in the LEARNING state
LAN Port <port #> is now in the FORWARDING state
```

SYSTEM OVERVIEW

SecureFast Virtual Remote Access Connection Manager (SFVRA-CONN or SFVRA Connection Manager) provides a rich set of network configuration, management, and reporting capabilities. It is implemented where network administrators require centralized control over a decentralized network. It is ideally suited for Internet Service Providers (ISP's), or for corporations implementing telecommuting or connecting their corporate, branch and remote offices.

SFVRA-CONN represents a new approach to managing a distributed network. It uses a Microsoft® SQL Server, and is implemented via client-server architecture. Client-server architecture has proven to be a highly effective means of implementing a wide range of computer-based applications.

SFVRA-CONN consists of an administration program and a user interface and runs with a database and a standard SQL Server. Every call made to a Remote Access Switch is validated against the database of users. A record of every call is stored in this central database. All calls can be viewed in a log of current calls and a log of past calls. Reports can be generated for support, billing or trend analysis. SFVRA Connection Manager provides assistance to Help desk personnel by keeping a record of problems that users encountered while trying to connect. This information can be viewed from any workstation running the Client software. In addition, SNMP traps are generated to notify network administrators for security violations. Multiple instances of SFVRA-CONN with multiple copies of the database can be provided for load sharing and reliability.

THE SFVRA CONNECTION MANAGER NETWORK

When a remote site calls a Remote Access Switch, a CyberSWITCH, it sends identification, such as a system name, and a password or challenge to the CyberSWITCH. The Remote Access Switch passes the information on to SFVRA-CONN via a TCP connection. SFVRA-CONN finds the user in the database by searching for the system name (if provided) or the Ethernet address for Combinet Proprietary Protocol users. If the user is found, the password or challenge is verified and configuration information about the user is sent to the Remote Access Switch.

After receiving user verification from SFVRA Connection Manager, the Remote Access Switch sends another message to verify that the call is acceptable. SFVRA-CONN checks the database to make sure that the time of day is valid and that the user has not exceeded the call minutes for that day or for that month. The bandwidth limitation is also verified. If the user has exceeded the maximum bandwidth on the initial connection, the Remote Access Switch drops the call and reconnects using a bandwidth within the range allowed. However, if the user requires more bandwidth and the maximum has not been reached, the Remote Access Switch is instructed to establish another call. Lastly, SFVRA-CONN checks the channel the remote site used to make the call. If the channel is reserved for priority users, the connection is dropped and re-established by the Remote Access Switch on an appropriate line, if available.

SFVRA-CONN can store static IP routes for each user. For users who are allowed to be called by the CyberSWITCHES, SFVRA Connection Manager advertises their static routes so other devices will know how to call these users. However, when a remote user is connected to a Remote Access Switch, that Remote Access Switch also broadcasts the user's static routes. In order to resolve this double broadcast, SFVRA-CONN broadcasts a metric value of 16 for all users that have a current connection. Therefore the SFVRA-CONN's broadcasted routes appear "farther" than the routes

broadcasted by the Remote Access Switch and therefore the current connection is used by other devices, if necessary. When the user disconnects from the Remote Access Switch, the static routes are removed from the Remote Access Switch's broadcast.

SFVRA Connection Manager allows IP address pools to be configured centrally. It dynamically assigns an available address when a user connects. This becomes more advantageous as the number of users increases. The Remote Access Switches form a hunt group, which is a group of lines that are tried (hunted) in succession until one is available to make a call. If the first line is busy, the next line is automatically tried, and so on, until a free line is found.

SFVRA-CONN is aware of all current connections. It monitors each call with regard to the restrictions set for each user. If a restriction, such as the maximum minutes per call, is violated, SFVRA-CONN instructs the Remote Access Switch to disconnect the call.

UNIQUE SYSTEM FEATURES

SecureFast Virtual Remote Access Manager combines unique features that centralize a decentralized network. These features include:

- Bandwidth Agility
  The system dynamically controls the bandwidth in use between itself and PPP devices. This is accomplished by establishing and disconnecting calls. Only the types and number of lines available limit the number of calls. The system monitors the connections for utilization and will add and remove the connections based on user configurable parameters. As network bandwidth requirements increase or decrease, the system will automatically adjust network connections. Thus, your network costs will reflect the actual bandwidth being used.

- Call Back
  If calls are required to be made from the central site to the remote site, for security or billing purposes, SFVRA Connection Manager provides automatic call back. After a remote user calls the central site, SFVRA-CONN will disconnect the call and re-establish the connection from a locally managed CyberSWITCH.

- Call Detail Recording
  The system compiles information for all current and past calls. It also presents a spreadsheet of calls that failed, including an explanation of the failure.

- Call Restriction
  SFVRA Connection Manager allows the administrator to limit the amount of call minutes accumulated for a remote site and limit access based on time of day for each user.

- Centralized Management
  All remote systems are configured on one database and the entire system may be monitored locally or remotely.

- Device and User Level Authentication
  This feature provides device level authentication by the SFVRA Connection Manager service while also requiring user level authentication from an off node authentication server, such as RADIUS, ACE, or TACACS.

- High Availability
  SFVRA Connection Manager will initiate a connection to a remote device in the event that an existing connection to that remote device is lost due to a failure of a locally managed CyberSWITCH.

- Load Leveling
  Incoming calls are evenly distributed between all available CyberSWITCHES within a hunt group.

- Network Security
  The Remote Access Switch ensures proper authentication (PAP, CHAP, CLID, NT or CPP) by validating the remote system with SFVRA database.

- Pooling
  Pooling can be configured system wide resulting in a large decrease of the amount of IP addresses needed.

- Protocol Discrimination
  It is possible for multiple types of remote devices to use the same line. The system can determine the device type and the protocol encapsulation used by remote devices.

- User Discrimination
  Network Administrators can reserve the last analog or digital connections of a specific Remote Access Switch for specific users. This provides priority for mission-critical personnel.

INTEROPERABILITY OVERVIEW

"Interoperability" is the ability to operate and exchange information in a heterogeneous network. The SFVRA Connection Manager supports interoperability with many different remote devices over ISDN.

INTEROPERABILITY PROTOCOLS

In order to communicate with various remote devices over ISDN, the SFVRA-CONN must identify the device type and the line protocol it is using.

The line protocols supported are:
- Combinet Proprietary Protocol (CPP) Ethernet Frames
- Point-to-Point Protocol (PPP) Encapsulation for IP Datagrams

Specific protocols within the line protocols are described in the CyberSWITCH documentation.

INTEROPERABILITY DEVICES

The remote devices that connect to the SFVRA Connection Manager can be classified into five types:

- MAC Layer Bridges
- IP Host Devices
- IP Router Devices
- IPX Routers
- AppleTalk Routers

MAC layer bridges connect to the Remote Access Switches using the CPP bridge encapsulation line protocol. These devices send transparently bridged Ethernet frames to the Remote Access Switches. MAC layer bridges do not process network layer protocols. They forward all packets based on source and destination MAC addresses.

IP Host devices are single workstations or PCs that connect to the Remote Access Switches at the IP network layer. These devices use either the RFC1294 based protocol or PPP to communicate with the Remote Access Switches.

IP router devices are single devices that represent many other IP hosts and routers to the Remote Access Switches. They must use the CHAP or PAP protocol to identify themselves to the system. IP routers usually provide IP network address information at connection time (and use PPP to send user data to the Remote Access Switches).

IPX routers are single devices that perform network layer tasks (addressing, routing and switching) to move packets from one location on the network to another. IPX routers use the Internetwork Packet Exchange (IPX) protocol, typical of the NetWare environment.

AppleTalk routers route AppleTalk datagrams based on address information. They support the following protocols: RTMP, NBP, and ZIP.

REMOTE ISDN DEVICES

The SFVRA Connection Manager provides a centralized concentrator function for remote ISDN devices. The devices can be separated into the following categories:

- Remote ISDN bridge devices
- PC based terminal adapters
- ISDN enabled workstations
- other ISDN routers

Typical remote ISDN bridges provide one Ethernet port and one Basic Rate ISDN port. The Basic Rate port is connected to the switched digital network and is used to make connections to the Remote Access Switch. The Ethernet port is used to connect to a remote LAN. The remote bridge device sends Ethernet frames from devices on the remote LAN over the switched network.

PC-based terminal adapters connect to a remote personal computer and use the switched digital network to connect to the system. The terminal adapter sends network protocol specific frames from the host PC device over the switched network.

Workstation-based terminal adapters connect to a workstation and use the switched digital network to connect to the system. The terminal adapter sends network protocol specific frames from the workstation over the switched network.

SYSTEM COMPONENTS

The major components of SFVRA Connection Manager are:

DATABASE

The database is a standard SQL Server that allows the system administrator to generate custom SQL Queries to retrieve and process data. The database stores the user configuration data, authentication data, and run time statistics.

CLIENT

The client is the graphical user interface used by the system administrator to configure and manage the system.

SFVRA SERVICE

The SFVRA Service performs the remote device authentication, call management, and connection logging functions.

RIP SERVICE

The RIP Service advertises static IP routes for remote devices. The RIP service only advertises for users that are connected or callable.

PROXY ARP SERVICE

The proxy ARP Service generates ARP replies for remote devices. This flattens the network topology by making remote devices appear to reside on the local segment.

BEFORE YOU INSTALL SFVRA CONNECTION MANAGER

Because SFVRA-CONN can administer access to thousands of users, planning your policies and topology is essential for success. The next sections discuss system requirements, policies that you should define, and how to position your SFVRA Connection Manager system.

SYSTEM REQUIREMENTS

To ensure reliable service and optimal performance, your system should meet certain physical requirements. This section identifies components of an ideal hardware system on which to run SFVRA-CONN.

SERVER PC REQUIREMENTS

For optimal performance, we recommend:

- 100 MHz Pentium™ PC
- 32-64 MB RAM
- 200 MB free disk storage (includes database)
- Windows NT® 3.51 with service pack 2 or Windows NT 4.0
- Microsoft SQL Server 6.0 or higher with 32-bit ODBC drivers
- Local network connection to managed CyberSWITCH systems
- Keyboard, mouse, and monitor

CLIENT PC REQUIREMENTS

- 33/66 MHz 486-class PC
- 8 MB RAM
- 2 MB free disk space
- Windows NT 3.51 with service pack 2 or higher, or Windows 95®
- Network connection to SQL Server
- 32-bit ODBC drivers
- Keyboard, mouse, and color monitor

POLICIES FOR CONFIGURATION

When you are planning to provide a dial-in service for remote users, there are important policies to define in order to configure it successfully.

- Device level security should be used for all remote users. This is generally PAP or CHAP for PPP users and CPP for combinet users. Windows NT security may be used to authenticate the remote user's password. SFVRA-CONN allows CLID to be used individually or in combination with other types of security.

- If there is more than one CyberSWITCH with pooling enabled, you should carefully design the use of hunt groups for the ISDN lines. If the hunt group spans the system, bandwidth should be restricted from remote sites to a single B-channel. This restriction ensures that another connection is not made from another Remote Access Switch to support the additional bandwidth. In addition, each Remote Access Switch should be configured with the same system name, PAP password, CHAP secret and IP WAN interfaces, so that the remote site is not aware of the Remote Access Switch on which the connection was established.

- IP addresses for subnets and individual hosts should be assigned based on the following criteria:

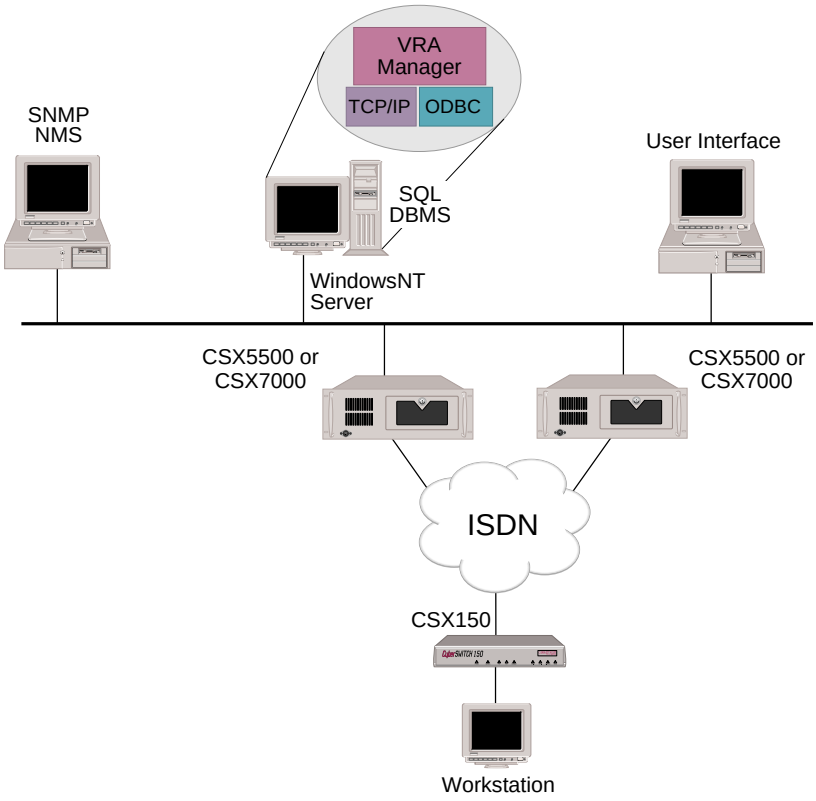
    - Are the interfaces on the WAN numbered or unnumbered? Make sure that all remote users support unnumbered before choosing it.

    - Can RIP v.2 be used to advertise routes at the central sites? Many other venders' routers do not support this version. If RIP v.1 must be used, the same subnet mask is recommended for all subnets.

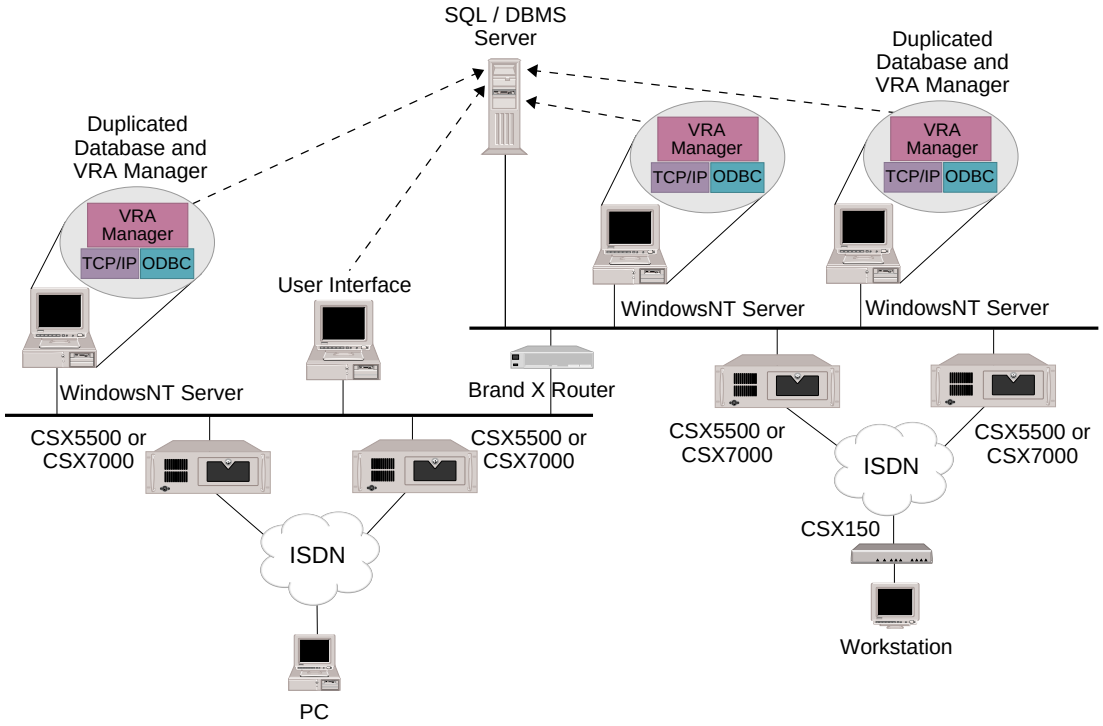
    - Are individual hosts going to be assigned addresses statically or will they be assigned dynamically when they connect? Dynamic assignment is preferred because it preserves addresses, but it can be used only for dial-in users.

NETWORK TOPOLOGY

SFVRA Connection Manager systems are normally positioned at the central site, attached to the enterprise backbone. NT Servers should be accessible by all the CyberSWITCHES through interconnected LANs or dedicated lines. You may want to position them behind firewalls to protect their valuable information.



We recommend that the SQL Server and SFVRA-CONN systems run on the same machine. However, if they are not run on the same machine, SFVRA-CONN system programs should be able to reach the SQL Server with minimal delay.



SFVRA Connection Manager is designed to provide a "fault tolerant" environment. Network administrators can implement multiple instances of SFVRA-CONN running on multiple machines. These instances can communicate with each other to provide dynamic resource assignment, such as load balancing. The databases themselves can be duplicated in real-time using the replication services of the leading SQL database engines.

You may want to have regional centers for Remote Access Switches that are connected via dedicated or switched circuits. Define these connections locally on the Remote Access Switches, while all other users are authenticated remotely using SFVRA-CONN.

SYSTEM INSTALLATION

The SFVRA Connection Manager consists of four components: the Client, which is the user interface to the database; the services, which control the Agents by the TCP/IP connection based on the information stored in the database; the Agents, which are the Remote Access Switches; and the Database. You also need an Open Database Connectivity (ODBC) software driver to connect each of the components, and an NDIS driver for the SFVRA RIP Service and the SFVRA Proxy ARP Service

This chapter provides instructions for installing the SFVRA Connection Manager system, and we also include instructions for installing the Adobe Acrobat Reader. You will need this reader to view the SFVRA-CONN user documentation.

INSTALLING THE SFVRA CONNECTION MANAGER SYSTEM

You must perform the following steps to install the SFVRA-CONN system.

1. Install the MS SQL Server
2. Install the ODBC Driver Pack 3.0
3. Install the SFVRA-CONN Software
4. Install the SFVRA Database
5. Install the NDIS driver

The following sections include instructions for performing each step.

INSTALLING THE MS SQL SERVER

Install the MS SQL Server according to the manufacturer's instructions. Ensure that the MS SQL Server Service is running.

INSTALLING THE ODBC DRIVE PACK 3.0

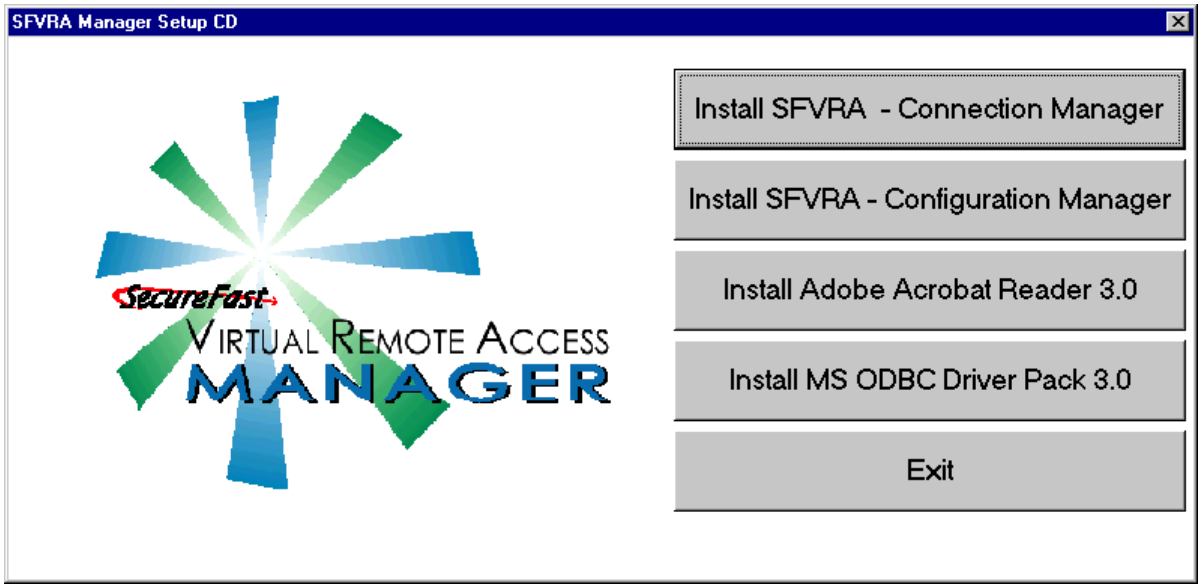
Each service for SFVRA Connection Manager requires a connection to the SQL Server. The components are connected by a set of software drivers called the ODBC (Open Database Connectivity). The ODBC hides the type of server, the location of the server, and the network protocol used to access the server from the application. This is an important feature because it gives the administrator the ability to control exactly how database is being used at any time. SFVRA-CONN requires the use of a 32-bit ODBC driver.

If the database is on a different IP subnet than the Client interface, SFVRA Service, RIP Service, and Proxy ARP Service, the ODBC drivers for these components must be configured to use IP rather than NetBEUI. To use IP transport protocols, a Network Library and a Network Address must be defined. If you are utilizing the password protection mechanism provided by the SQL Server, you must use either the LMHOSTS file or WINS to resolve the server name to an IP address. Simply configuring the ODBC Network Address will not be sufficient to read the remote registry.

Complete the following ODBC set-up on each device that will run any component of the SFVRA Connection Manager application and on the device containing the MS SQL Server.

1. Close any active applications.

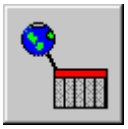
2. Insert the SFVRA Manager Setup CD into the CD-ROM drive. If, as is usually the case, your CD-ROM is setup for AutoRun, the following screen will automatically load:



   To manually load the above screen, select *Run* from the Start Menu. Enter *<CD-ROM drive>:\SCCD.EXE* as the program to open, then select *OK*.

3. From the initial install shield screen (shown above) click *Install ODBC Drive Pack 3.0*.

4. When prompted, choose the *Complete Install* option.

5. If installation fails, repeat the above steps, however, choose the *Custom*  option instead of *Complete Install*.
   a. Ensure that *SQL Server* and *ODBC components* are selected.
   b. Deselect *Desktop Drivers* and *Oracle* by clicking in the respective boxes.

6. If the Data Sources window is displayed during the installation of the ODBC Driver Pack click *System DSN* and then select to *add* a data source; otherwise, once the installation of the ODBC Driver Pack completes, open *32-bit ODBC* from the Control Panel, click *System DSN*, and select to *add* a data source.

7. Select the *SQL Server* driver. Click *OK*.

8. Enter *SFVRA* for the *Data Source Name.*

9. For *Server*, select the device on which the SQL Server was installed.

Note: If the database is on a different IP subnet, steps 10 and 11 are necessary for configuration. If the database is on the same subnet, skip to step 12.

10. Enter an IP address as the *Network Address* of the machine on which the database resides.

    Note: The IP address of the machine on which the database resides may also be configured in the LMHOSTS file or using WINS.

    - LMHOSTS file configuration
      Enter the IP address of the SQL Server with the server name in the c:\winnt\system32\drivers\etc\LMHOSTS file. The entry shown below allows the system to resolve a NetBIOS name to an IP address.
      1.1.1.1 Server_Name

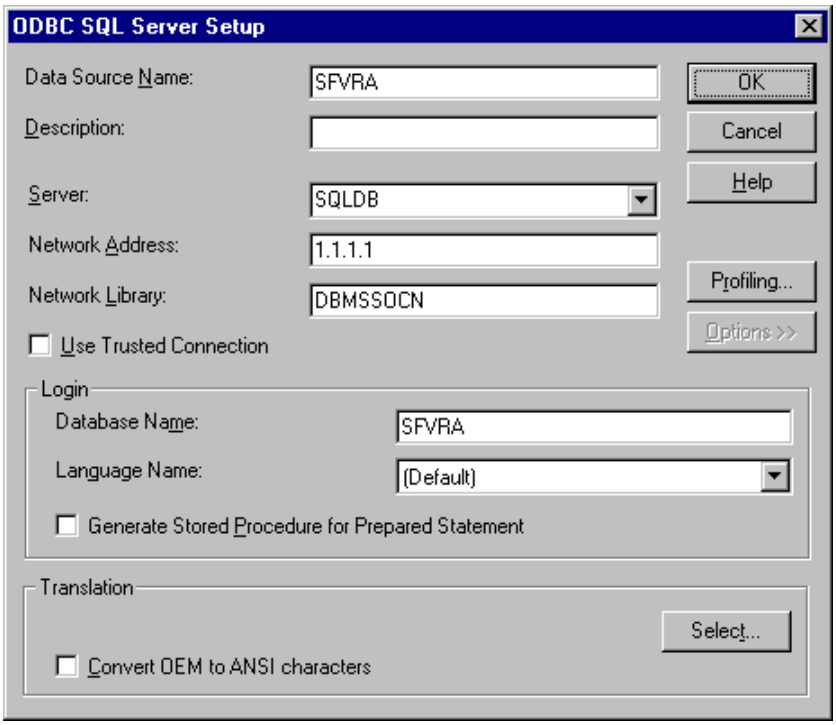
    - WINS configuration
      Register the SQL Server machine and the remote machine with the same WINS Server. The remote machine must disable LMHOSTS checking in the WINS Server configuration. The procedures for creating, configuring and maintaining a WINS Server are beyond the scope of this document. Consult the Windows NT system documentation for these procedures.

11. Enter ***DBMSSOCN*** as the *Network Library*.

    Note: The DBMSSOCN.DLL file may be obtained from the Microsoft SQL Server CD-ROM. This file should be saved in the c:\winnt\system32 directory.

12. Click *Options*. Enter ***SFVRA*** for the *Database Name*. Deselect *Generate Stored Procedure for Prepared Statement*.

The ODBC SQL Server Setup dialog should appear as follows:



13. Click *OK* and then click *Close*.

INSTALLING THE SFVRA-CONN SOFTWARE

Install the SFVRA Connection Manager software on a Windows NT device, preferably on the same device as the MS SQL Server. The Client software may be installed on a Windows 95 or Windows NT device. During the software installation, you will be given the option of installing:

- Client Files includes the software for the Client Interface, the Manage Logins application, the CSX Monitor application, and the Convert application.
- SQL Setup application aids in the creation of SFVRA database files for the Microsoft SQL Server. The SQL Setup application should only be installed on the PC running the MS SQL Server.
- Service Files includes the SFVRA Service, the SFVRA RIP Service, and the SFVRA Proxy ARP Service.
- The SFVRA Connection Manager Documentation installs the User's Guide.

Install the SFVRA-CONN software using the following steps:

1. Ensure that ODBC setup has been performed on the systems.

2. Close any active applications.

3. Insert the SFVRA Manager Setup CD into the CD-ROM drive. If, as is usually the case, you CD-ROM is setup for AutoRun, the initial installation screen will be displayed.

   To manually load the screen, select *Run* from the Start Menu. Enter `<CD-ROM drive>:\SCCD.EXE` as the program to open, then select *OK*.

4. From the initial installation screen click *Install SFVRA Connection Manager*.

   Note: Installation and configuration of SFVRA Configuration Manager is discussed in a separate manual.

5. At the prompt, determine whether the SFVRA Database and MS SQL Server are installed on this machine.

6. Follow onscreen instructions to complete the installation.

INSTALLING THE SFVRA DATABASE

The SFVRA Connection Manager uses Microsoft (MS) SQL Server (6.0 or later) for its database. Install this database on a Windows NT device. The SFVRA Database is created by the SQL Setup Utility. You may choose to run this utility when installing SFVRA-CONN software. If you choose not to run the utility while installing the software you may start the utility after completing the software installation. The following instructions briefly discuss the set up of the SFVRA Database. Refer to the *SQL Setup Utility* chapter for more information.

1. Login to the MS SQL Server. Enter the Login ID `sa` and a password, if necessary, and click *OK*. The SQL Setup program executes.

2. The SQL Setup Utility informs you of the processes it will accomplish. Click *Continue*.

3. Specify the device size. We recommend specifying the device size of at least 20 MB. Click *Create*.

4. Once the SFVRA Device has been created, the SQL Setup will create the SFVRA database, groups, login and users. Click *Create*.

5. After the SFVRA Database has been successfully created, the SQL Setup will create database tables. Click *OK*. This procedure may take several minutes, since the SQL Setup runs an ISQL script.

6. When the SQL Setup program has finished, MS SQL Server messages are listed in the dialog box. Ensure that no error messages are listed in the *SQL Server Messages* dialog. Click *Close*.

INSTALLING THE NDIS DRIVER

The SFVRA RIP Service and SFVRA Proxy ARP Service require the use of an NDIS driver. Install this driver on any machine that runs one of these services.

1. From the Control Panel, open *Network*.

For Windows NT **3.51**:

2. Click *Add Software*.

3. Select <*Other*> *requires disk from manufacturer*. Click *Continue*.

For Windows NT **4.0**:

2. Click *Add* on the *Protocols* tab.

3. Click *Have Disk*.

For both Windows NT **3.51** and **4.0**:

4. Enter the path `c:\Program Files\SFVRA\Service`. Click *OK*.

5. Select *NDIS 3.0 Packet Driver v3.5*. Click *OK*.

   Note: After the driver is installed, it is listed as Network Express Driver on the *Service* dialog.

6. Click *Close* and restart the machine when prompted.

INSTALLING THE SIMPLE NETWORK MANAGEMENT PROTOCOL

The SNMP Agent allows the SFVRA Connection Manager system to be monitored from a local and / or remote Network Management Station (NMS). The SNMP Agent will only generate traps from the SFVRA-CONN. Traps are protocol data units that transmit problem information. These problems are similar to those listed in the problem log with some exceptions. For example, if a call were rejected based on an authentication failure, a trap would be immediately sent to the NMS. Traps are also sent if any of the Remote Access Switches go down. However, traps are not sent when a User is disconnected based on a time restriction. SNMP is in compliance with IP, however since the SFVRA-CONN determines the traps that are sent, the NMS also receives information for non-IP servers. If you choose to set up a Network Management Station, follow the instructions below on installing and configuring the SNMP Service.

INSTALLING WINDOWS NT SNMP SERVICE

1. From Control Panel, open *Network.*

For Windows NT **3.51**:

2. Click *Add Software.*

3. Select *TCP/IP Protocol and related components.* Click *Continue.* Select *SNMP Service.*

For Windows NT **4.0**:

2. Click *Add* on the *Services* tab.

3. Select *SNMP Service.* Click *Have Disk.*

For both Windows NT **3.51** and **4.0**:

4. Locate the Windows NT distribution files, or insert the original Setup disks. Click *Continue.*

5. Restart machine when prompted.

CONFIGURING THE SNMP SERVICE

1. From the Control Panel, open *Network.*

For Windows NT **3.51**:

2. Select *SNMP Service* from the *Installed Software* dialog. Click *Configure.*

For Windows NT **4.0**:

2. Select *SNMP Service* from the *Network Services* window.

For both Windows NT **3.51** and **4.0**:

3. Enter the *Community Name* from which the traps will be sent and enter the *IP address* of the SNMP Network Management Station which will receive these traps.

   Note: Additional help can be obtained from the Control Panel's help buttons.

COMPILING THE MIB FILE

After installing and configuring the SNMP Service, SFVRA-CONN will generate and send specific traps. However, in order for the NMS to properly view these traps, the SFVRA.MIB file must be compile on the NMS. The process for compiling this file depends on the NMS that you are using. Refer to the instructions on compiling MIB files for your specific NMS. The SFVRA.MIB is located in the c:\Program Files\SFVRA\Service directory.

INSTALLING ADOBE ACROBAT READER

To review or print the SFVRA Connection Manager documentation, you will need Adobe Acrobat Reader. We have included the Reader setup utility on this CD for those of you who do not already have a version of Reader.

To install Adobe Acrobat Reader:

1. Close any active applications.

2. Insert the SFVRA Manager Setup CD into the CD-ROM drive. If, as is usually the case, your CD-ROM is setup for AutoRun, the initial installation screen will be displayed.

3. On the SFVRA Manager Setup CD initial installation screen, click on *Install Adobe Acrobat Reader 3.0*.

4. Follow the onscreen instructions to complete the installation.

To view the SFVRA-CONN documentation:
From the Start Menu select Programs\SFVRA, then select *SFVRA Documentation*.

USING THE SFVRA-CONN APPLICATION

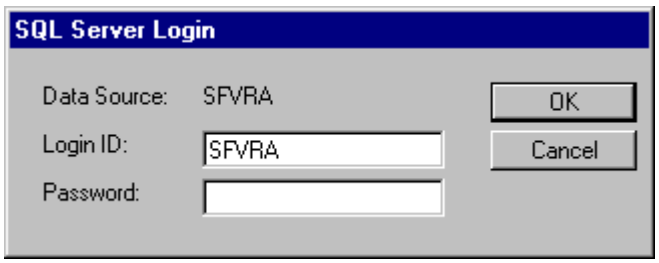
OVERVIEW

This chapter includes the following sections:

- Starting the SFVRA-CONN Client
  This section provides instructions for starting up the SFVRA-CONN Client application.
- SFVRA Service
  This section describes the operation of the SFVRA Service.
- RIP Service
  This section describes the operation of the RIP Service.
- Proxy ARP Service
  This section describes the operation of the Proxy ARP Service.
- Starting and Stopping the SFVRA-CONN Services
  When using the SFVRA-CONN application you may need to start or stop the operation of one or more services. This section steps you through this process.

STARTING THE SFVRA-CONN CLIENT

1. From the Start menu\Programs\SFVRA, select *SFVRA*. The SFVRA-CONN Client program executes.
2. From the *File* menu, select *Connect*, or click on the toolbar to connect to the database.
3. A dialog similar to the following will be displayed:



Note: The first time you use the SFVRA-CONN Client application, the login ID is set to SFVRA. If desired, you may edit this field to change the login ID. You must have read / write privileges to make changes in the Client application. However, read only login accounts may view the Client information. Refer to the *Manage Logins* chapter for more details.

4. If required, enter your password.

5. Click *OK*.

SFVRA SERVICE

The SFVRA Service must establish a connection to the database before it will perform any authentication, management or logging functions. Once the database connection is established, the SFVRA Service will open connections to the CyberSWITCH systems that are configured in the database. When a connection has been established to a CyberSWITCH, the service begins the process of user authentication, call management and connection logging.

In a traditional system, the user authentication procedure includes call management and data logging functions. However, these functions have been split into separate operations in order to provide flexibility in the usage of the SFVRA-CONN system.

Authentication is provided at the device level. If SFVRA Service has been selected to perform authentication, call management and data logging are also performed. Call management consists of ensuring that the time of day that the remote device attempts to connect is valid, as well as maintaining a limit on the number of call minutes for each call, day and month. Data logging tracks current calls as well as past calls. Data logged includes the time of connection and disconnection per device, as well as other useful information, such as maximum bandwidth, the type and direction of the call. A problem log reports lost connections and the reason for their termination.

The SFVRA Service uses a standard ODBC connection to the SQL Server. The SQL Server may reside on the same machine as the SFVRA Service or on another machine that is accessible via the LAN. Although there is a nokeepalive mechanism to ensure that the database connection is active, the SFVRA Service has been designed to recover from a database connection failure.

The CyberSWITCH systems and the SFVRA Service communicate through a TCP/IP connection. The standard TCP/IP keepalive mechanisms are too slow to be useful in maintaining the connection between a CyberSWITCH and the SFVRA Service. Therefore, the SFVRA-CONN protocol specifies keepalive messages that are used to maintain the connection. If no messages have been received from the CyberSWITCH for 5 seconds a keepalive message is sent.

If three consecutive keepalives fail, no response received from a CyberSWITCH, the connection is closed. The SFVRA-CONN will set the status of all active calls on the CyberSWITCH to "UNKNOWN", and will try to reconnect every 45 seconds.

Upon establishment of a connection between a CyberSWITCH and the SFVRA Service, the SFVRA Service will request a User Audit Reply message from the CyberSWITCH. The User Audit Reply is a message that specifies every active ISDN or Digital Modem call on the CyberSWITCH. The SFVRA Service uses this message to ensure that the Database and the SFVRA Service tables match the CyberSWITCH state.

The User Audit Request, which request the current state of the connections, is used to prompt the CyberSWITCH for a User Audit Reply. The SFVRA Service sends a User Audit Request to the CyberSWITCH at the following times:

1. A connection has just been established between the CyberSWITCH and the SFVRA Service.
2. A connection has just been established between the Database and the SFVRA Service.
3. Once per hour.

RIP SERVICE

The RIP Service must establish a connection to the database. Once the database connection is established, the RIP service will get the set of groups to which it belongs. The RIP Service then downloads the static routes for all remote devices that belong to the same groups as itself. It gets the IP addresses of the SFVRA Services from the database and opens a connection to the SFVRA Services through a TCP/IP connection. When a connection has been established to an SFVRA Service the RIP Service begins the process of advertising routes for remote devices. The RIP service can advertise IP routes for the remote devices that are connected or callable.

PROXY ARP SERVICE

The Proxy ARP Service must establish a connection to the database. Once the database connection is established, the Proxy ARP Service then downloads the IP addresses and static routes for all remote devices which belong to the same group as itself. The Proxy ARP Service gets the IP address of the SFVRA Services from the database and opens a connection to the SFVRA Services through a TCP/IP connection. When a connection has been established to an SFVRA Service, the Proxy ARP Service begins the processing ARP requests.

The Proxy ARP Service receives all ARP requests on the network. For each ARP request, the service checks the IP addresses and the static routes of all connected devices, and checks the IP pool addresses currently in use for a match with the target IP address. If a match is found, a proxy ARP reply is sent using the MAC address of the connecting CyberSWITCH as the sender MAC address. If a match is not found, the service checks the IP addresses and static routes of all callable remote devices for a match with the target IP address. If a match is found, an ARP reply is sent using the MAC address of the local machine as the sender MAC address. This causes any subsequent IP packets destined for the target IP address to be sent to the Proxy ARP Service.

A similar procedure is used for receiving IP packets as well. Each IP packet received, the service checks the IP addresses and static routes of all connected remote devices, and checks the IP pool addresses currently in use for a match with the target IP address. If a match is found, the packet is discarded. If a match is not found, the service checks the IP addresses and static routes of all callable remote devices for a match with the target IP address. If a match is found, a request is sent to the SFVRA Service to establish a connection to the remote device. The IP packet is then placed into a list of pending IP packets. When a connection to the remote device is established, the SFVRA Service notifies the ARP Service. If the connection is not established within 15 seconds the packet is discarded.

The SFVRA Service sends notification messages to the ARP Service whenever connections are established or terminated. When the ARP Service receives a connection notification message, it

marks the remote device as connected. It then checks the destination IP addresses in the list of pending IP packets for a match with the remote device's static routes or IP address. If a match is found, the ARP Service broadcasts a gratuitous ARP for the destination IP address with the CyberSWITCH'S MAC address as the sender MAC address. This causes all local devices to update their ARP cache entry for this IP address, if they have such an entry.

Note: The Default Gateway of the machine where the Proxy ARP Service resides must be configured as its own IP address. To configure the Default Gateway, follow the steps outlined below:

1. From the *Control Panel*, open *Network*.
2. Select the TCP / IP Protocol and click *Properties*.
3. Configure the Default Gateway to be the same as the IP Address.
4. Click *OK*. Restart the machine, if necessary.

STARTING AND STOPPING THE SFVRA-CONN SERVICES

At times you may want to start and / or stop the SFVRA Connection Manager services. This requires the following steps.

1. From the *Control Panel*, open *Services*.
2. Select one of the following services: *SFVRA ARP Service*, *SFVRA RIP Service*, or *SFVRA Service*.

   Note: The Proxy ARP Service must be started manually. If you are using the Proxy ARP Service we suggest that you make this service automatic.

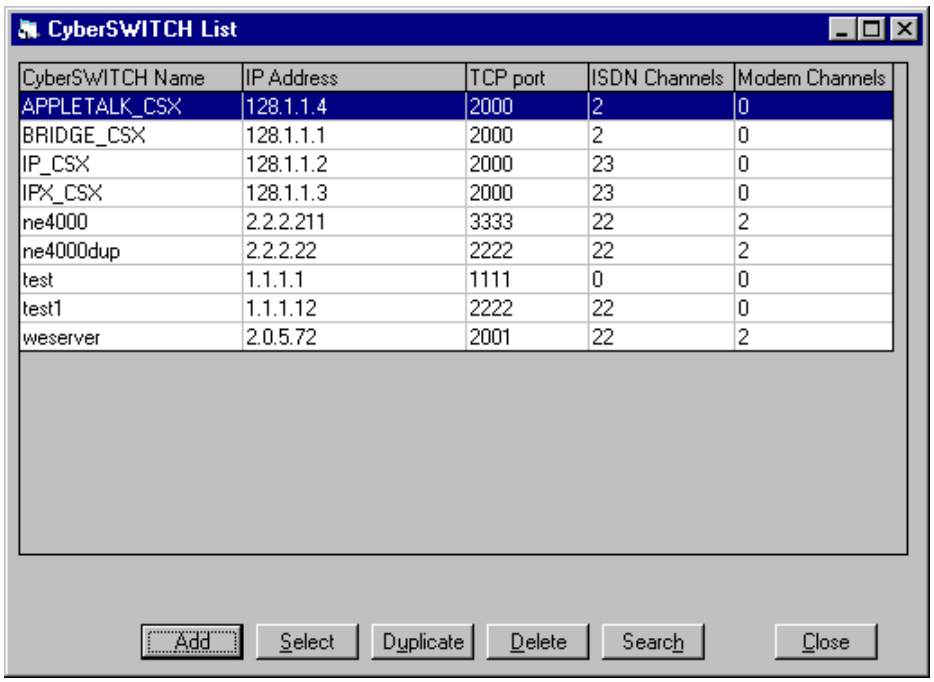
3. Click *Start* or *Stop* for the desired operation.
4. Click *Startup* if required.
5. Select a Startup Type of *Automatic* or *Manual*. Click *OK*.
6. Click *Close*.

CONFIGURING REMOTE ACCESS SWITCHES

OVERVIEW

The SFVRA Connection Manager provides you with the capability to configure, update and collectively view several basic features about the Remote Access Switches connected to it. Each CyberSWITCH, a Remote Access Switch, needs to be configured individually, and care must be taken to ensure similar configurations between the CyberSWITCH and SFVRA-CONN. Since a proprietary authentication protocol is used, SFVRA-CONN only operates with the Cabletron CyberSWITCH family of remote access products. This chapter provides information for configuring basic features of the CyberSWITCHES for SFVRA-CONN. These features are:

- CyberSWITCH basic properties
- Reserving a B-channel for priority users
- Creating a pool of addresses

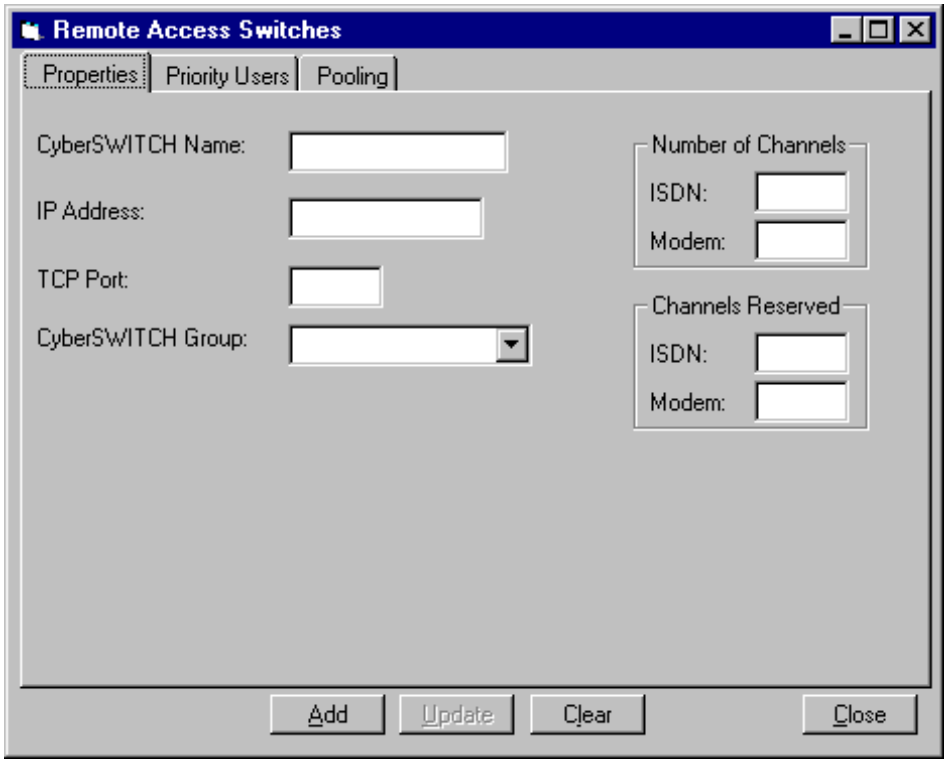


CYBERSWITCH LIST
An alphabetical list of currently configured CyberSWITCHES.

CYBERSWITCH PROPERTIES

The Properties tab displays the basic configuration parameters of the CyberSWITCH. For configuration, each Remote Access Switch must have a unique name and IP address. A unique-to-the-Remote Access Switch TCP port number is also required for communication with SFVRA Connection Manager. CyberSWITCHES may only belong to one group or no groups. See *Configuring CyberSWITCH - User Groups* for more information.

The number of channels is based on hardware availability. Check adapters to find the number of ISDN and Digital Modem lines that are available. Channels Reserved indicates the number of B-channels that will be available only to Priority Users.



CYBERSWITCH NAME

A name used to uniquely identify this CyberSWITCH in the SQL Database. This name is mandatory and must be unique, however, it doesn't have to match the System Name configured on the actual CyberSWITCH.

IP ADDRESS

The IP address of the Remote Access Switch's LAN port through which a TCP connection may be established to the SFVRA-CONN.

TCP PORT

The TCP port used by the SFVRA-CONN to communicate with the CyberSWITCH. Note that you can assign a user-defined port number, but that the SFVRA-CONN TCP port number must be entered identically on both the CyberSWITCH and the SFVRA-CONN.

CYBERSWITCH GROUP
This feature allows CyberSWITCH systems and users to be grouped together to manage which CyberSWITCH systems are available to each user.

NUMBER OF CHANNELS
The number of ISDN and / or Digital Modem channels which the Remote Access Switch currently supports. These numbers are based on the hardware configuration of the Remote Access Switch. This feature is optional for adding a CyberSWITCH, however, connections can not be made to the CyberSWITCH unless the numbers of channels is greater than zero.

CHANNELS RESERVED
The number of ISDN and / or Digital Modem channels that are reserved for use only by priority users that are designated on the Priority User's table. This number can not exceed the number of channels configured for the CyberSWITCH. This feature is optional.

CONFIGURING REMOTE ACCESS SWITCH PROPERTIES

1. On the *Functions* menu, select *CyberSWITCH,* or click on the toolbar. The *CyberSWITCH List* dialog appears.

2. Select a CyberSWITCH that which you want to configure Properties, or click *Add* to configure a new CyberSWITCH. The *Remote Access Switches* dialog appears.

3. Select the *Properties* tab.

4. Enter a unique name for the CyberSWITCH. The name does not need to match the System Name configured on the CyberSWITCH.

5. Enter the IP Address, using dotted decimal notation, of the Network Interface on the CyberSWITCH through which a TCP connection may be established to the SFVRA-CONN.

6. Enter the TCP Port number on the Ethernet-2 resource to which the physical LAN for interface corresponding to the IP Address is connected.

7. Optional: select a previously configured CyberSWITCH - User Group.

   Note: CyberSWITCHES may only belong to one group.

8. Enter the number of ISDN and / or Digital Modem channels configured for the CyberSWITCH based on its hardware configuration.

9. Optional: enter the number ISDN and / or Digital Modem channels that are reserved for Priority Users.

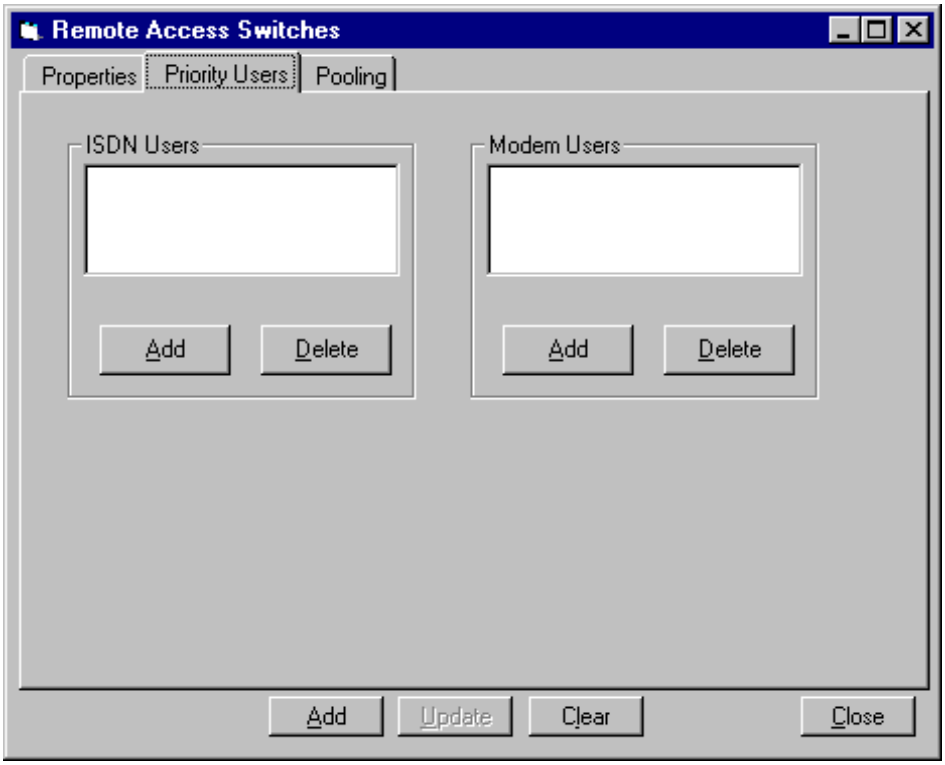
10. Click *Update* to write the new information for the CyberSWITCH to the database, or click *Add* to create the newly configured CyberSWITCH.

11. Click *Close*.

Note: Additional information about configuring the CyberSWITCH systems themselves can be found in the CyberSWITCH documentation.

PRIORITY USERS

Some remote users are more critical than others. These users can be designated as priority users, which reserves the last available B-channel for the priority user only. Reserving channels is an optional feature. You can select users, whether they are ISDN or modem users, to have access to the reserved B-channels. Users must be properly configured for Dial Out before they are made available as Priority Users.



ISDN USERS
Lists ISDN users within the same group as the currently selected CyberSWITCH that have been selected as Priority Users.

MODEM USERS
Lists Digital Modem within the same group as the currently selected CyberSWITCH users that have been selected as Priority Users.

CONFIGURING PRIORITY USERS

1. On the *Functions* menu, select *CyberSWITCH*, or click on the toolbar. The *CyberSWITCH List* dialog appears.

2. Select a CyberSWITCH that which you want to configure Priority Users. The *Remote Access Switches* dialog appears.

   Note: Configuring Priority Users for a CyberSWITCH can only be done in the *Update* mode.

3. Select the *Priority Users* tab.

4. Click *Add* for either ISDN or Digital Modem, depending upon the type of user you would like to add to the priority user list.

   Note: Users must be previously configured on the SQL database before they can be designated as priority users. Refer to the *Configuring Users* chapter for more information. The list of users displayed includes only those that have been configured as ISDN or Modem users, respectively, and that are in the same group as the CyberSWITCH.

5. Select the user that you want to be a Priority User and click *OK*.

6. Click *Update* to write the new information to the database.

7. Click *Close*.

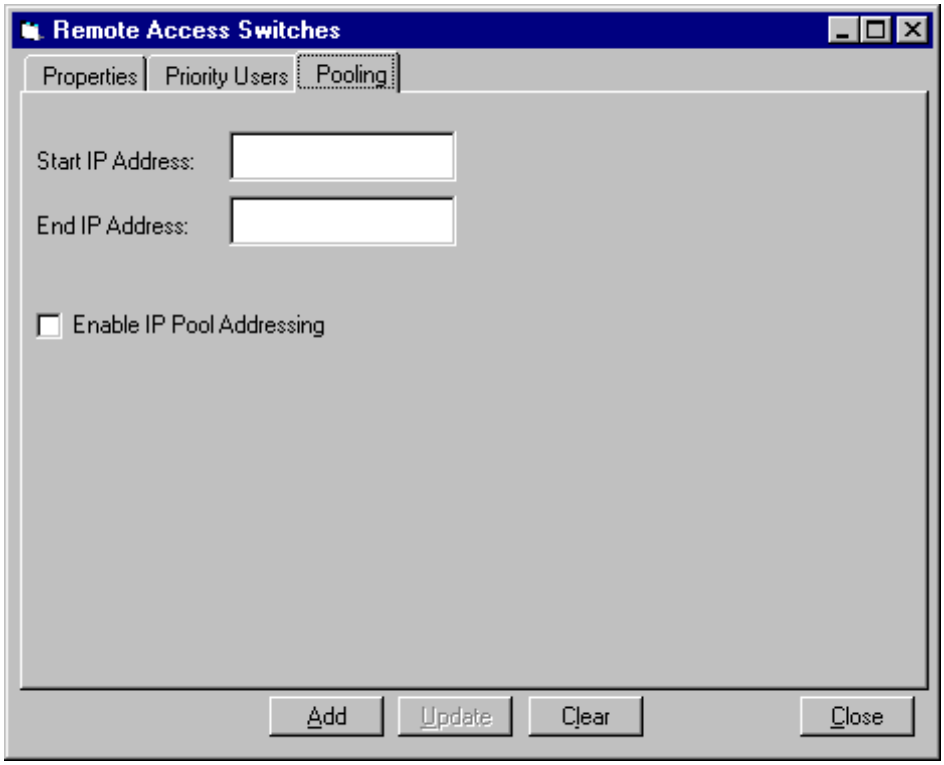
POOLING

The IP Address Pool feature allows you to configure a list of IP addresses that can be dynamically assigned to remote IP devices as they connect to the CyberSWITCH. This occurs when a remote IP device calls in to the CyberSWITCH and has no IP address, and requests to have one assigned. With this capability, you no longer need to assign permanent IP addresses to all possible remote IP devices, but rather only as many IP addresses as the number of possible ISDN connections. If multiple connections are used, you would not need as many IP addresses as the number of possible ISDN connections. This can result in a reduction of the number of IP addresses required for remote IP users.

When a PPP connection is established to a Remote Access Switch, the Remote Access Switch and the remote device exchange their IP addresses during the IPCP (IP Control Protocol) phase. If the remote device does not know its own IP address, SFVRA Connection Manager will assign a proper IP address to it. A proper IP address can be a permanent IP address configured for the remote device in the user table, or it can be one of the IP addresses configured in the IP Address Pool. If an IP address from the address pool is used, it will be returned to the pool when the connection is terminated. This allows the IP address to be reused for other remote IP devices.

Remote Access Switches supporting the IP Pool feature form a hunt group for the users. We suggest restricting bandwidth to a single B-channel for remote sites. Each CyberSWITCH within the hunt group should be configured with the same CyberSWITCH name, password, secret, and IP WAN interfaces, so the remote user dialing in is not aware of the CyberSWITCH on which the connection was established. This feature is optional.

Note: An IP address should not be configured for the user (either locally or in SFVRA-CONN) if an IP address is to be assigned to the user from the IP address pool.



START IP ADDRESS

The Start IP Address field designates the beginning of a range of IP addresses that are used by this CyberSWITCH to assign IP addresses to any user that does not already have an IP address configured. The range is inclusive. An address is required before enabling the IP Pool. IP addresses should be entered in the dotted decimal notation: "XXX.XXX.XXX.XXX".

END IP ADDRESS

The End IP Address field designates the end of a range of IP addresses that are used by this CyberSWITCH to assign IP addresses to any user that does not already have an IP address configured. The range is inclusive. An address is required before enabling the IP Pool. IP addresses should be entered in the dotted decimal notation: "XXX.XXX.XXX.XXX".

ENABLE IP POOL ADDRESSING

Enables IP Pooling for this CyberSWITCH. The Start and End IP Addresses must be configured before enabling this feature. IP Pool Addressing must be disabled before reconfiguring the start and / or end addresses. This feature dynamically assigns IP addresses to participating users.

CONFIGURING REMOTE ACCESS SWITCH POOLING

1. On the *Functions* menu, select *CyberSWITCH*, or click on the toolbar. The *CyberSWITCH List* dialog appears.

2. Select a CyberSWITCH that which you want to configure an IP Address Pool, or click *Add* to configure a new CyberSWITCH. The *Remote Access Switches* dialog appears.

3. Select the *Pooling* tab.

4. Enter a *Start IP Address*. This address is included in the range.

5. Enter an *End IP Address*. This number is included in the range.

   Note: The range of addresses should be limited to the same subnet.

6. Click *Enable IP Pool Addressing*.

7. Click *Update* to write the new information for the CyberSWITCH to the database, or click *Add* to create the newly configured CyberSWITCH.

   Note: If you are adding a new CyberSWITCH to the database, a CyberSWITCH Name, IP Address, and TCP Port Number must be defined on the *Properties* tab.

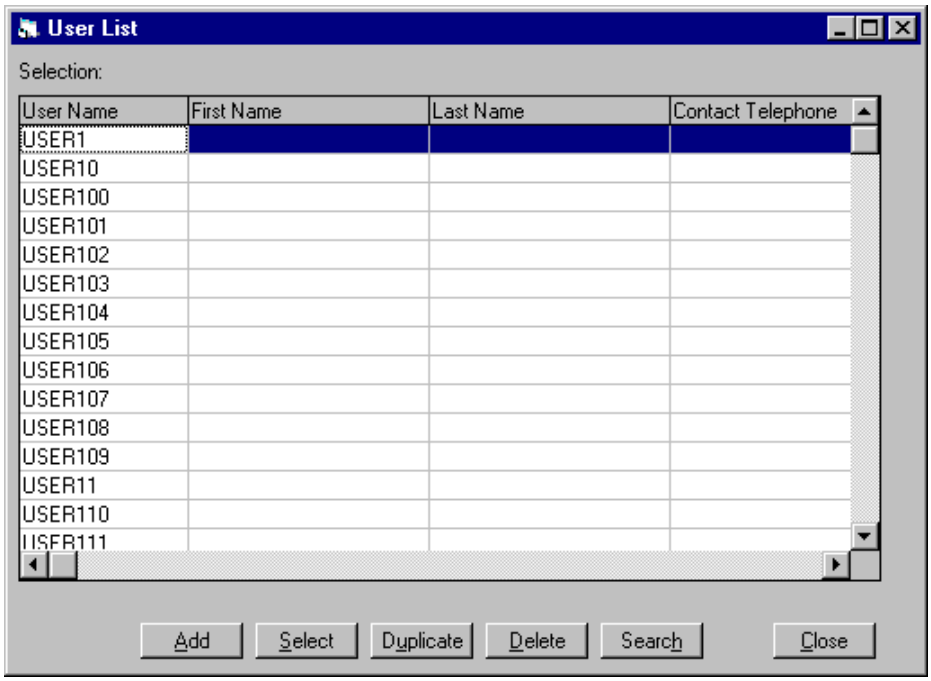
8. Click *Close*.

CONFIGURING USERS

OVERVIEW

User Records is a set of valid remote devices that can access the network resources by connecting to one of the Remote Access Switches and replaces the On-node Device Database. User Records contains a symbolic name for the user and a unique identifier that is used to enforce user security. Since the Remote Access Switches refer to SFVRA Connection Manager whenever a connection is attempted, all users are configured on SFVRA Connection Manager, rather than on each Remote Access Switch. For each type of remote user added to the database, you must have previously configured a corresponding network interface on each CyberSWITCH that the user can access. User Records contains the following information:

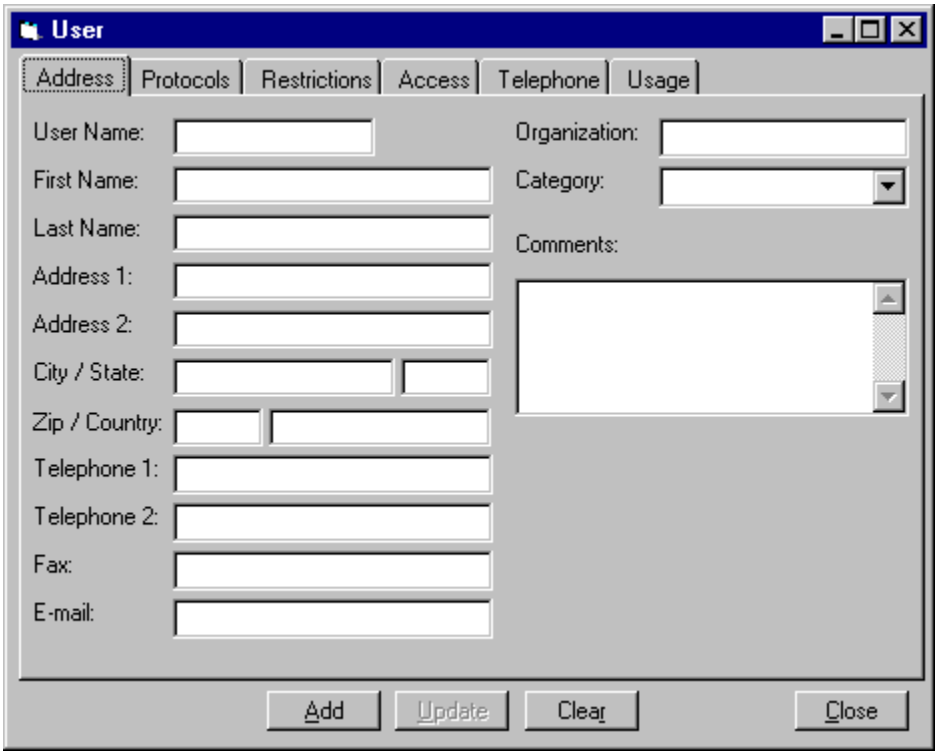
- User address and contacts
- Protocols
- Time and bandwidth restrictions
- Access security
- Dial out configurations
- Call usage



USER LIST
An alphabetical list of currently configured users.

ADDRESS

Each user is required to have a unique User Name. The name (first and last), address (location and e-mail), organization, relevant numbers (telephone and fax), and any comments are optional features within User Records. This information can be used as a contact person to remote devices. Included in this feature is a SFVRA Connection Manager administrator defined category. Remote devices can be categorized and accessed by this category through the functions of the database.



USER NAME

A name used to uniquely identify a user, a remote device, in the SQL Database. The User Name must match the name configured at the remote device.

FIRST AND LAST NAME

The first and last name of the user, or the person responsible for the user. This feature is optional.

ADDRESS

The address of the user, or the person responsible for the user. This feature is optional.

TELEPHONE

The telephone numbers of the user, or the person responsible for the user. This feature is optional.

FAX

The Fax number of the user or the person responsible for the user. This feature is optional.

E-MAIL

The E-mail address of the user, or the person responsible for the user. This feature is optional.

ORGANIZATION
The organization to which the user, or the person responsible for the user, belongs. This feature is optional.

CATEGORY
The category of the user, or of the person responsible for the user. This feature is optional, but categories must be previously defined. Categories are configured through the Tables menu.

COMMENTS
This field is for storing any comments or special information that pertains to the user or the person responsible for the user. This feature is optional.

CONFIGURING USER ADDRESS

1. On the *Functions* menu, select Users, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure the Address features, or click *Add* to configure a new user. The *User* dialog appears.
3. Select the *Address* tab.
4. Enter a *User Name*.
5. The remaining information is optional, but is available to store useful information. The category of the user needs to be previously configured in order to be available. See *Configuring User Categories* for further information.
6. Click *Add* to write the new information to the SQL database.
7. Click *Close*.

CONFIGURING USER CATEGORIES

1. On the *Tables* menu, select *User Categories*. The *Table Maintenance* dialog appears.
2. Click *Add*, and provide a new entry.
3. Click *OK* to write the new category to the SQL database.
4. Click *Close*.

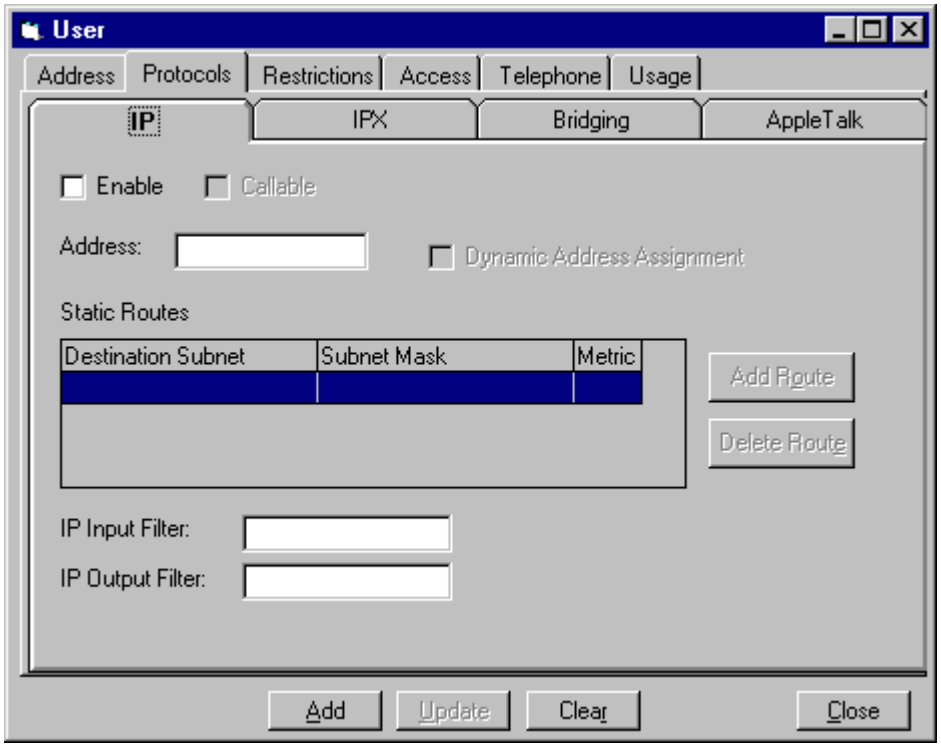
PROTOCOLS

In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Determine whether the user communicates by IP, IPX, bridge, AppleTalk, or a combination.

IP

When IP is enabled, the CyberSWITCH acts as a router, routing IP datagrams based on IP address information to the user. The default configuration is IP disabled.

Note: If the bridge and the IP options are enabled, the SFVRA-CONN will instruct the CyberSWITCH to act as a brouter. A brouter operates as a router for protocols it can route, and operates as a bridge for protocols it cannot route.



ENABLE

Enabling IP indicates that the user is an IP Router and that the CyberSWITCH connected to it should route IP datagrams to the user based on IP network layer information.

CALLABLE

Callable indicates that a Remote Access Switch is to initiate connections to this user based on an IP packet. This feature is available only if IP is enabled, and the user is properly configured for dial out. This feature cannot be used with Dynamic Address Assignment.

ADDRESS

The IP address of the remote device. Use 0.0.0.0 to indicate an UnNumbered Interface. This feature is only available if IP is enabled.

Notes: If you change the IP address under the *Bridging* protocol selection, this parameter will reflect that change.

This field can also be used to specify an IP (Sub-)Network Number for bridge devices connecting to Remote LAN interfaces.

DYNAMIC ADDRESS ASSIGNMENT
Indicates that this user will be assigned an IP Address by a Remote Access Switch when the user dials in to the CyberSWITCH. This feature will only work properly if at least one Remote Access Switch that can reach the user has enabled the IP Pool.

IP INPUT FILTER
An IP Input Filter monitors packets that this user sends into SFVRA-CONN's local subnet. The filter must be previously defined on the Remote Access Switches. Undefined filters will be ignored.

IP OUTPUT FILTER
An IP Output Filter monitors packets that this user receives out from the SFVRA-CONN's local subnet. The filter must be previously defined on the Remote Access Switches. Undefined filters will be ignored.

CONFIGURING THE IP PROTOCOL

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure for the IP protocol, or click *Add* to configure a new user. The *User* dialog appears.
3. Select *IP* on the *Protocols* tab.
4. *Enable* IP by clicking in the box.
5. Determine if the user is *Callable*.

   Note: A telephone number through which a CyberSWITCH can establish a connection must be configured before enabling the callable function. See *Configuring Telephone*.

6. Enter the *IP Address* of this user, or enable *Dynamic Address Assignment* so that the user will be assigned an address upon connecting with a CyberSWITCH.
7. Optional: enter an *IP Input Filter*.
8. Optional: enter an *IP Output Filter*.
9. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

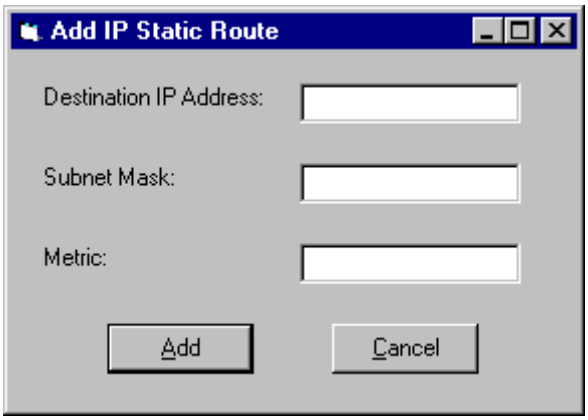
   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.

10. Click *Close*.

Note: An IP Network Interface must be defined on all Remote Access Switches that each IP user can access. Refer to the *IP Network Interfaces* section in the CyberSWITCH documentation for further information.

STATIC ROUTES

Static routes may be configured for each user. Static routes specify the IP address of the next hop router or gateway that provides access to the user's network. You only need to configure a static route if the user needs to access a LAN or WAN network that is not directly connected to any of the Remote Access Switches administered by SFVRA Connection Manager and the Remote Access Switches cannot or will not exchange routing information with the next hop device. A CyberSWITCH cannot exchange routing information if the user does not RIP across the shared network or if the CyberSWITCH is using an UnNumbered IP interface to communicate with the user. A CyberSWITCH will not exchange routing information if RIP is disabled by the administrator, such as is often done over dial-up WAN links.



DESTINATION SUBNET

IP address using dotted decimal notation that specifies the destination (sub-) network.

SUBNET MASK

The Subnet mask for the destination (sub-) network. Entering the number of contiguous bits that are set for the mask specifies the Subnet mask. The mask bits start at the most significant bit of the IP address field and proceed to the least significant bit. The user is assigned a mask automatically based on the class of the Destination Subnet, but it may be reconfigured if the default is not desired. A Subnet mask of 255.255.255.255 implies that this static route entry is for a host rather than a (sub-) network.

METRIC VALUE

The administrative distance to the destination of the entry. The number of hop counts (number of routers) typically measures the administrative distance between the SFVRA-CONN and the destination, but it is up to you to assign proper value to each route entry. If multiple routes exist to the same destination, the route with the least metric value will be chosen as its primary route. The range of metric values for static routes is from 1 to 16.

You may manipulate the metric value to promote a certain default route, or to impede a default route from being used. For example, if there is a route that in reality has several hops, but they are all over LAN connections, you may want to assign a low metric to this route so that a route is taken that is local, thus, no toll charges. Or, perhaps there is a route with a low number of hops, but the connection is over a WAN. You may want to assign this route a high number of hops to limit toll charges, in case there is a local route that could be used.

Configuring Static Routes

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a User that which you want to configure static route(s). The *User* dialog appears.

   Note: The user must be added to the database before static routes are configured.
3. Select *IP* on the *Protocols* tab.
4. See *Configuring the IP Protocol* if the user has not been configured for IP.
5. Click *Add Route.*
6. Enter the *Destination Subnet*.
7. Accept the default *Subnet Mask*, or enter a new one.
8. Enter the *Metric* value.
9. Click *Add* on the *Add IP Static Route* dialog.
10. Click *Update* to add the static route(s) for the user to the database.
11. Click *Close*.

IPX

IPX protocol accepts data from remote devices and formats the data for transmission onto the network, and conversely, accepts data from the LAN and formats it so remote devices can understand it. In short, IPX allows remote devices and their servers to communicate.

The SFVRA-CONN supports the standard method of routing datagrams over a network. The system provides bandwidth management features to make the interconnection of IPX networks cost effective over demand type connections like ISDN. Additional security features provide data privacy for networks using IPX that are connected by the system.

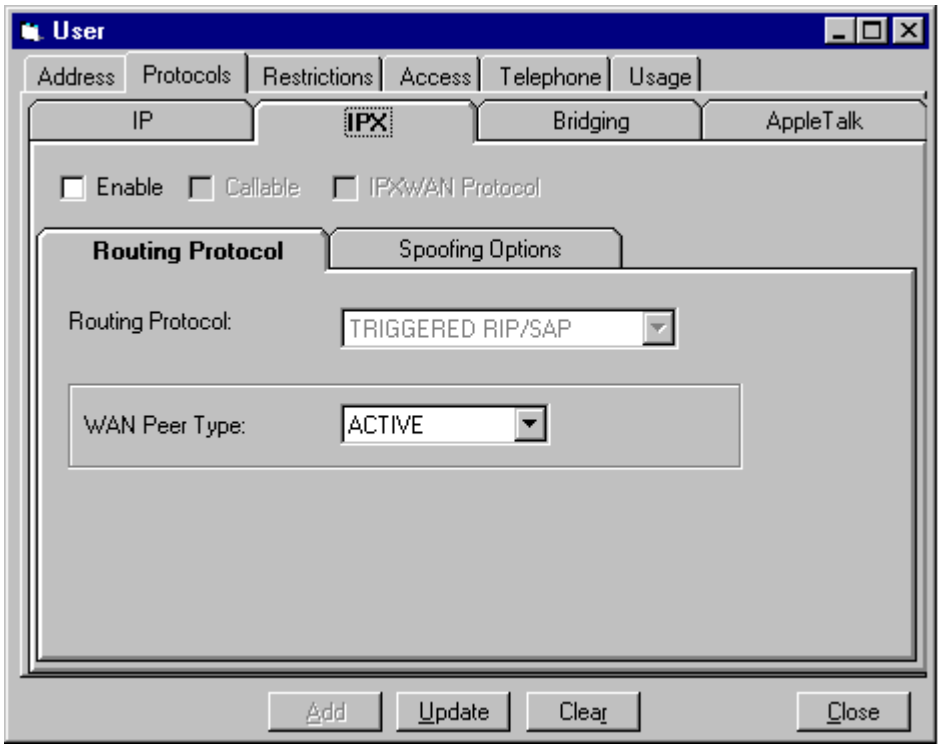
IPX Option Background Information

The Internetwork Packet Exchange (IPX) protocol is a datagram, connectionless protocol in the NetWare environment analogous to the Internet Protocol (IP) in the TCP / IP environment. With the help of Routing Information Protocol (RIP) and Service Advertising Protocol (SAP), the IPX router performs the network layer tasks of addressing, routing and switching information packets, to move packets from one location to another in a complex network.

The SFVRA-CONN supports the standard method of routing Novell® IPX datagrams over an internetwork. The system provides bandwidth management features to make the interconnection of IPX networks cost effective over demand type connections like ISDN. Additional security features provide data privacy for Novell networks connected by the system.

Over the last few years Novell has evolved their WAN IPX routing model. Originally the Novell IPX router supported numbered WAN network interfaces only. That is, a unique IPX network number was assigned to each WAN port on the router.

Novell then migrated to an unnumbered WAN network interface in their latest versions of their IPX router. When two routers communicate, they will try to use the unnumbered network interface type. If both routers support this type of interface they will agree on this and initiate data transfer. If one router does not support the unnumbered type, the newer router will defer to the older router and agree to use a numbered type interface. The new router will let the older router assign the network number for the WAN link.



ENABLE
Enabling IPX indicates that the user is an IPX Router and the CyberSWITCH connected to it should route IPX datagrams to this user based on IPX network layer information.

CALLABLE
Callable indicates that a CyberSWITCH is to initiate connections to this user based on an IPX packet. This feature is valid only if IPX is enabled, and the user is properly configured for dial out.

IPX WAN PROTOCOL
Enabling the IPX WAN Protocol indicates that this user is an IPX router and that the IPX WAN protocol must immediately succeed IPXCP negotiations. The options negotiated in IPXCP will be replaced by these negotiations. If IPX WAN protocol is disabled, the IPX packets will start flowing as soon as IPXCP negotiations are completed.

ROUTING PROTOCOL

Indicates the protocol the user will be using to communicate with the CyberSWITCH.

- NONE specifies no routing protocol. Static routes and services must be configured on each CyberSWITCH in the same group as the user.
- RIP/SAP allows the periodic broadcast of routing and service information across WAN circuits.
- Triggered RIP/SAP specifies a modified version of RIP/SAP, in which information is broadcasted on the WAN only when there has been as update to the database or a change in the reachability of a next hop router.

WAN PEER TYPE

This feature distinguishes how to handle triggered RIP/SAP information, and is only available when Triggered RIP/SAP has been selected as the routing protocol. An Active Peer receives broadcasts and conveyed information at all times. A Passive Peer receives broadcasts and conveyed information only when a connection is up between the CyberSWITCH and the user.

CONFIGURING THE IPX PROTOCOL

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

2. Select a user that which you want to configure for the IPX protocol, or click *Add* to configure a new user. The *User* dialog appears.

3. Select *IPX* on the *Protocols* tab.

4. *Enable* IPX by clicking in the box.

5. Determine if the user is *Callable.*

   Note: A telephone number through which a CyberSWITCH can establish a connection must be configured before enabling the callable function. See *Configuring Telephone*.

6. Enable the *IPX WAN Protocol* if desired.

7. Select the desired *IPX Routing Protocol.*

8. If *Triggered RIP/SAP* is chosen as the *Routing Protocol*, select the desired *WAN Peer Type* for the user.

9. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.

10. Click *Close*.

Note: An IPX Network Interface must be defined on all Remote Access Switches that each IPX user can access. Refer to the *IPX Network Interfaces* section in the CyberSWITCH documentation for further information.

IPX SPOOFING

NetWare was designed for the LAN environment, and assumes that there is always available bandwidth. Because of this, NetWare protocols are not well suited to WANs. Special handling must be given to the NetWare protocols to prevent them from causing excessive ISDN connections. The special handling of NetWare protocols in a routing environment consists of spoofing and automatic filters.

Spoofing is a method to prohibit excessive ISDN connections by internally generating a desired response packet when a request packet is received that should be routed over the WAN and there is no connection up to the remote user. The NetWare protocols that require spoofing to be performed are the Watchdog Protocol and the Sequence Packet Exchange (SPX) Protocol. Automatic filters are also used to prohibit excessive ISDN connections caused by the NetWare protocols.

Watchdog Protocol

Watchdog Protocol is used by NetWare Servers to detect “dead” clients. If a server has seen no traffic from an attached client for a configurable amount of time, the server sends a watchdog packet to the client to determine if the client is still alive or merely inactive. If, after a few minutes, a server does not receive a watchdog reply, it is assumed that the client is no longer alive and the connection to the server is terminated.

If no connection exists to a user and the server sends a watchdog request to a remote client, a connection would have to be established to deliver the watchdog request. With watchdog spoofing enabled, a watchdog response is generated internally and delivered to the server as if the remote client sent the packet. This satisfies the server without causing a connection to be established. To allow a server to timeout a client that is no longer alive, the watchdog requests are forwarded over the WAN when a connection already exists. In addition, a watchdog spoofing duration time, T, can be specified. When the connection is down to a user and a watchdog request is received that should be forwarded to this user, a watchdog response will be spoofed for T amount of time. After T amount of time, the watchdog request will be filtered without generating a response. The duration timer T starts when a user is disconnected and is reset each time a new connection is established.

This above described implementation will be followed for watchdog request packets received over the LAN and the WAN. If a watchdog request is received over the WAN and it is determined that a spoofed watchdog response should be generated, it will be returned over the same WAN connection on which it was received.

The implementation of watchdog spoofing eliminates unnecessary connections while allowing clients to be aged out and does not require any client side spoofing or end-to-end-protocol.

The parameters for watchdog spoofing are configured for each remote user. The watchdog spoofing option can be enabled or disabled. By default the option is enabled. When disabled the watchdog requests are routed without any special handling. If the option is enabled, the watchdog spoofing duration time T is specified in minutes. The default is set to 120 minutes.

SPX Protocol

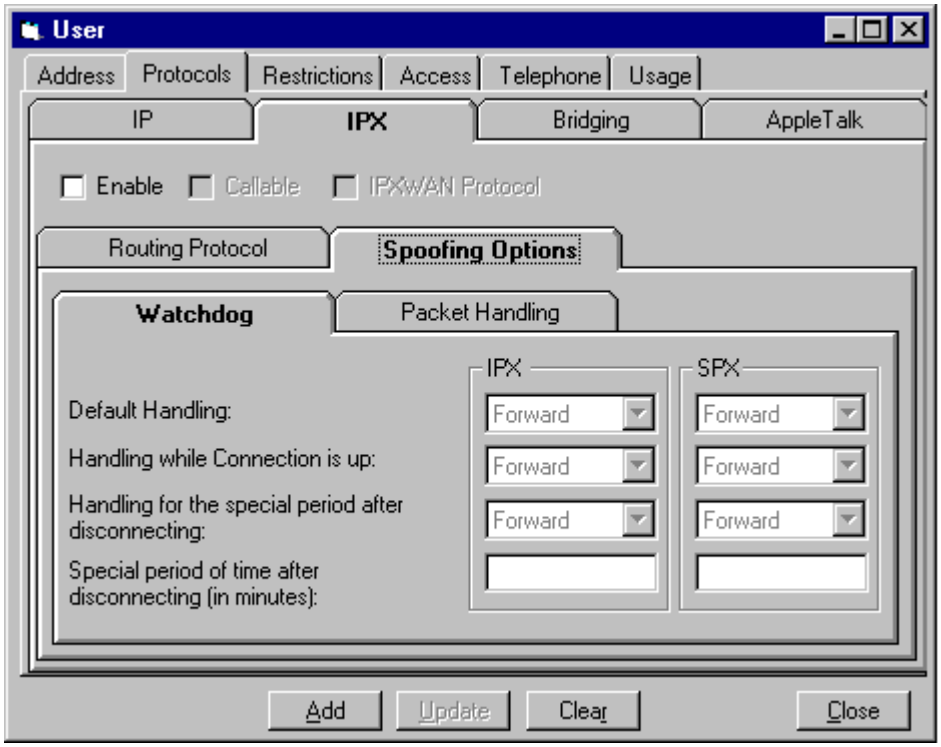
SPX Protocol is optionally used by NetWare applications requiring guaranteed, in-sequence delivery of packets by a connection-oriented service. Each end of an SPX connection sends keep-alive packets, identified as <SYS> packets, to monitor the status of the connection.

The SPX protocol ensures connection integrity by exchanging a keep-alive packet between the connection end-points, once every 6 seconds. If an SPX keep-alive packet is received that is destined for a remote user and no connection exists to the user, a connection would have to be established to deliver the packet. The keep-alive packets are handled using the same approach being used for server watchdog request packets. With SPX spoofing enabled, a keep-alive is generated internally and delivered to the local endpoint as if the packet was sent by the remote endpoint. This satisfies the local endpoint without causing a connection to be established. To allow an SPX connection to timeout the keep-alives are forwarded over the WAN when a connection already exists. In addition, an SPX spoofing duration time T can be specified. When the connection is down to a user and a keep-alive is received that should be forwarded to this user, a keep-alive will be spoofed for T amount of time. After T amount of time, the keep-alive will be filtered without generating a keep-alive response. The duration timer T starts when a user is disconnected and is reset each time a new connection is established.

Some of these <SYS> packets are overloaded in that they are not just keep-alive packets but are control packets needed for the application to run successfully and hence have to be routed like regular SPX data packets. If any NetWare application does not seem to work across WANs, it may be because of the mishandling of these <SYS> packets and can be traced by disabling SPX keep-alive spoofing.

This above described implementation is followed for keep-alive packets received over the LAN and the WAN. If a keep-alive is received over the WAN and it is determined that a spoofed keep-alive should be generated, it will be returned over the same WAN connection on which it was received.

The parameters for SPX spoofing are configured for each user. The SPX spoofing option can be enabled or disabled. By default the option is enabled. When disabled the SPX keep alives are routed without any special handling. If the option is enabled the SPX spoofing duration time T is specified in minutes. The default is set to 120 minutes.

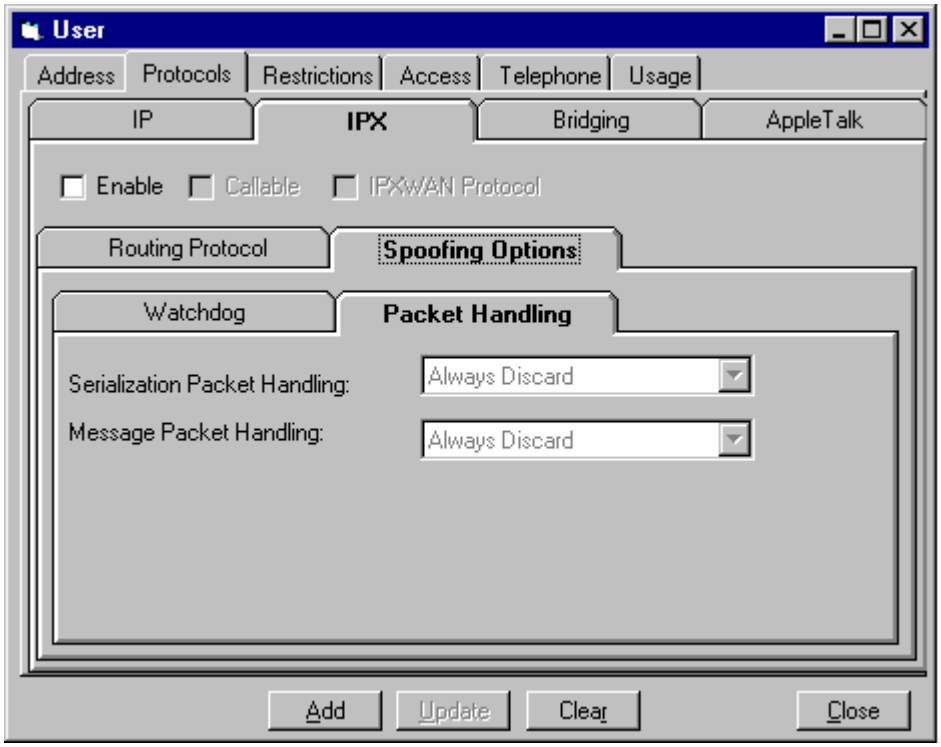


DEFAULT HANDLING
Determines how a CyberSWITCH should handle Watchdog Spoofing and SPX packets when there is no connection established to the user.

HANDLING WHILE CONNECTION IS UP
Determines how a CyberSWITCH should handle Watchdog Spoofing and SPX packets while there is a connection to the user.

HANDLING FOR THE SPECIAL PERIOD AFTER DISCONNECTING
Determines how a CyberSWITCH should handle Watchdog Spoofing and SPX packets during the administrator defined special period after the user disconnects.

SPECIAL PERIOD OF TIME AFTER DISCONNECTING
Defines the length of the special period in minutes after disconnecting from this user. The special period is the amount of time that, after a remote bridge disconnects, the MAC Addresses on that bridge are retained.



SERIALIZATION PACKET HANDLING

Serialization packets are used to detect unauthorized duplication of NetWare Software. Servers send serialization packets to pass their serialization numbers to other servers to verify the server software has not been copied. By default the automatic filtering option for serialization packets is set to Always Discard.

MESSAGE PACKET HANDLING

Message Waiting packets are sent by servers to attached clients to inform them that the server has a message to send to them. When the server receives the reply to the message-waiting packet it sends the actual message to the client. The server will send another message waiting packet to the client every two seconds until it receives a response or until the connection with the client is terminated. By default the automatic filtering option for message waiting packets is set to Always Discard.

Configuring IPX Spoofing

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

2. Select a user that which you want to configure for the IPX Watchdog Spoofing, or click *Add* to configure a new user. The *User* dialog appears.

3. Select *IPX* on the *Protocols* tab.

   Note: If IPX has not been configured for this user, see *Configuring the IPX Protocol* for more information.

4. Select the *Spoofing Options* tab.

   Note: The Watchdog Spoofing and Packet Handling options are the same for both IPX and IPX RLAN. Changing the options on the IPX tab identically changes the options on the IPX RLAN tab, and vice versa.

5. Change any IPX or SPX watchdog spoofing options that you desire, or accept the defaults.

6. Select the *Packet Handling* tab.

7. Change any Packet Handling options that you desire, or accept the defaults.

8. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a User Name must be defined on the Address tab.

9. Click *Close*.

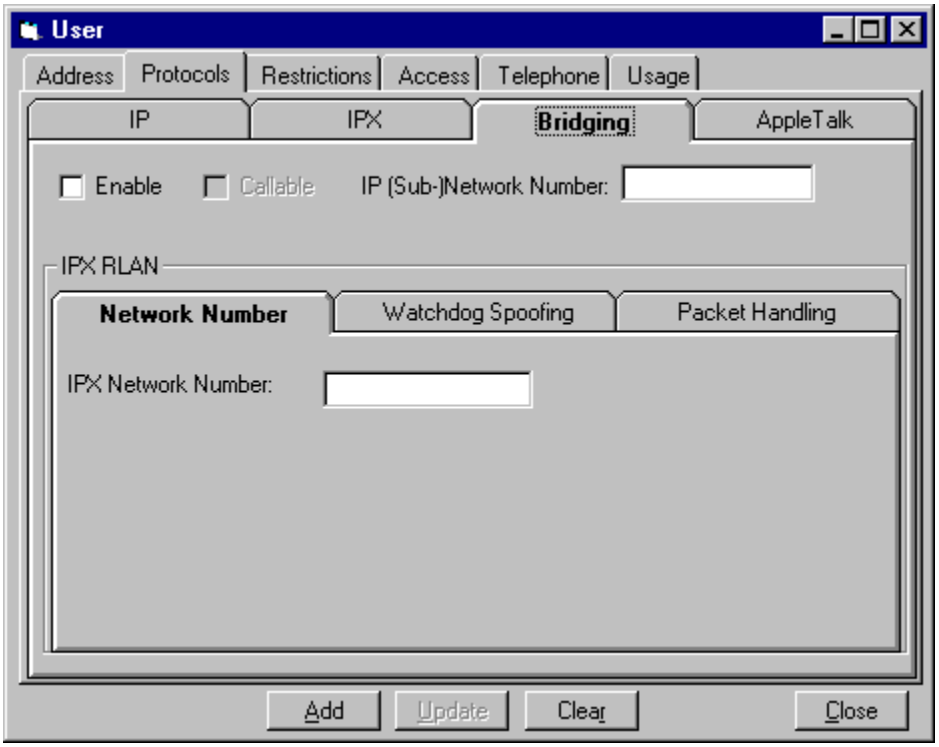
BRIDGING

You are given the option of either enabling or disabling the MAC layer bridging feature. When bridging is enabled, the CyberSWITCH bridges data packets to the proper destination, regardless of the network protocols being used.

Note: If the bridge and any of the routing protocols are enabled, the system will act as a "brouter." A brouter operates as a router for protocols it can route, and operates as a bridge for protocols it cannot route.

With bridging enabled, bridge dial out is supported. Bridge dial out, allows the SFVRA-CONN to initiate connections to bridge devices at remote sites. The system accepts bridge data received on the Ethernet LAN or ISDN network, and initiates a data connection to a bridge device specified in the user data.

The "bridge" determines if a connection already exists, or whether a connection should be initiated. The MAC frame is simply forwarded if a connection already exists. If a connection does not, the SFVRA-CONN will map the Bridge Address or User Name to a phone number, and initiate a connection. The normal connection processing, protocol negotiation, and data forwarding mechanisms are followed once the connection is requested.



ENABLE

Enabling Bridging indicates that the user is a Bridge and the CyberSWITCH connected to it should route Bridge datagrams to this user based on Bridge network layer information.

CALLABLE

Callable indicates that a CyberSWITCH is to initiate connections to this user based on a Bridge packet. This feature is valid only if bridging is enabled, and the user is properly configured for dial out.

IP (SUB-)NETWORK NUMBER

If the CyberSWITCH uses an IP RLAN interface to connect to a remote bridge, you must provide this information. This address associates the bridge with the IP network to which it connects. Enter this address using dotted decimal notation. This parameter applies to the network-portion of the IP address only. Note that if you change the IP address under the *IP* protocol selection, this parameter will reflect that change.

IPX NETWORK NUMBER

The IPX Network Number specifies the IPX network that is used on the remote LAN for the user. This hexadecimal number ranges from 1 to 4 bytes in length. None indicates that the remote LAN does not have an explicit IPX network number and will be associated with the first configured IPX RLAN interface on a CyberSWITCH.

CONFIGURING THE BRIDGING PROTOCOL

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure for the Bridging protocol, or click *Add* to configure a new user. The *User* dialog appears.
3. Select *Bridging* on the *Protocols* tab.
4. *Enable* Bridging by clicking in the box.
5. Determine if the user is *Callable*.

   Note: A telephone number through which a CyberSWITCH can establish a connection must be configured before enabling the callable function. See *Configuring Telephone*.
6. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.
7. Click *Close*.

IP REMOTE LAN

The WAN (Remote LAN) IP Network Interface allows remote MAC layer-bridge devices to connect to an IP subnet. The CyberSWITCH treats all devices connected to the RLAN IP Network Interface as if they were connected to the same Ethernet segment. The system provides an explicit IP router presence on this RLAN that is implemented over ISDN. IP Address Resolution requests are intelligently propagated to remote bridged networks connected on the RLAN IP network interface. The WAN (Remote LAN) IP Network Interface is used for CPP Bridge and PPP remote devices.

Configuring IP Remote LAN

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure for the IP RLAN options, or click *Add* to configure a new user. The *User* dialog appears.

   Note: If Bridging has not been configured for this user, see *Configuring the Bridging Protocol* for more information.
3. Select *Bridging* on the *Protocols* tab.
4. Enter the IP (Sub-) Network Number of the IP RLAN Interface.

5. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.

6. Click *Close*.

Note: A WAN (Remote LAN) IP Network Interface must be defined on all Remote Access Switches that each Bridging with IP RLAN user can access. Refer to the *IP RLAN Network Interfaces* section in the CyberSWITCH documentation for further information.

IPX REMOTE LAN

An IPX WAN (Remote LAN) interface can be used to connect remote bridge devices to the other IPX router network interfaces. The IPX router treats all bridge devices connected to the RLAN as if they were on an Ethernet LAN segment. A CyberSWITCH emulates an Ethernet medium over the series of ISDN point to point connections in order to accomplish this. The IPX router encapsulates IPX data for the RLAN interface in Ethernet packets and forwards the data to the remote bridges.

If the user has NetWare Clients attached to its remote LAN, these clients will assume the IPX network number assigned to the RLAN interface on the Remote Access Server. If the user has both NetWare servers and clients attached to its remote LAN, the clients will assume the IPX network number of the remote NetWare server. An explicit IPX Network Number needs to be configured for the user so that the same network number is applied to the remote LAN each time the user connects.

Note: IPX RLAN options are only available if Bridging is enabled and IPX is disabled.

IPX Spoofing on a RLAN Interface

In order to maintain NetWare server connectivity, some IPX packets require spoofing. This spoofing requires special handling by the IPX RLAN interface. The following rules apply to IPX spoofing on a RLAN interface.

1. If the destination MAC address is unknown, the packet cannot be spoofed. It will be treated as a normal packet and forwarded to all connected bridges in the RLAN.

2. If the destination MAC address is known, the configured spoofing parameters are applied to packets forwarded on the RLAN interface.

3. A MAC address will be known for the configured Special Period after Disconnecting spoofing parameter.

Note: Refer to the *IPX Spoofing* section for more information.

Configuring IPX RLAN

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure for the IPX RLAN options, or click *Add* to configure a new user. The *User* dialog appears.
3. Select *Bridging* on the *Protocols* tab.

   Note: If Bridging has not been configured for this user, see *Configuring the Bridging Protocol* for more information.
4. Enter an *IPX Network Number*, if necessary.
5. Select the *Watchdog Spoofing* tab.
6. Change any IPX or SPX spoofing options that you desire, or accept the defaults.
7. Select the *Packet Handling* tab.
8. Change any Packet handling options that you desire, or accept the defaults.

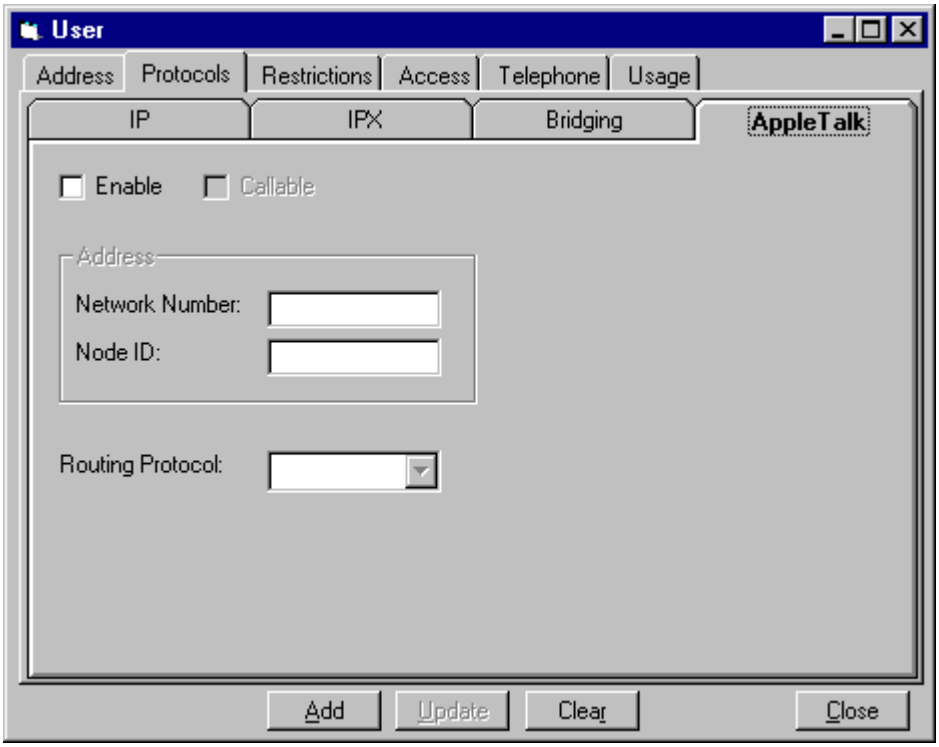
   Note: The Watchdog Spoofing and Packet Handling options are the same for both IPX and IPX RLAN. Changing the options on the IPX tab identically changes the options on the IPX RLAN tab, and vice versa.
9. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.
10. Click *Close*.

Note: A WAN (Remote LAN) IPX Network Interface must be defined on all Remote Access Switches that each Bridging with IPX RLAN user can access. Refer to the *IPX RLAN Network Interfaces* section in the CyberSWITCH documentation for further information.

APPLETALK

The Extended Network type indicates that the user is connected to an Extended AppleTalk network, which allows addressing of more than 254 nodes and supports multiple zones. The NonExtended Network type indicates that the user is connected to a NonExtended AppleTalk network, which supports addressing of up to 254 nodes and supports only one zone. SFVRA Connection Manager does not check the validity of the node number configured for each user.



ENABLE

This parameter indicates whether the user routes AppleTalk datagrams or not. When enabled, it indicates that the remote device will route AppleTalk datagrams. When disabled, it indicates that the remote device will bridge AppleTalk datagrams. Note that it requires AppleTalk RLAN feature to handle bridged AppleTalk datagrams, and therefore until AppleTalk RLAN is implemented, AppleTalk routing can not be used with remote devices that do not route AppleTalk.

CALLABLE

Callable indicates that a CyberSWITCH is to initiate connections to this user based on an AppleTalk packet. This feature is valid only if AppleTalk is enabled, and the user is properly configured for dial out.

NETWORK NUMBER

The AppleTalk network range (for Extended network) or the AppleTalk network number (for NonExtended network) of the LAN segment that the port is connected to. Specifying 0.0 (for Extended) or 0 (for NonExtended) places the port in discovery mode (a.k.a., non-seed router), in which the system learns its configuration information from the seed router. Note that there must

be at least one seed router on the network. Discovery mode is not supported for WAN ports, and therefore a valid network range/number needs to be specified.

NODE ID
If the system is acting as a seed router on this port, then this parameter specifies the suggested AppleTalk address (Extended) or Node Id (NonExtended), which is used as initial value for the AppleTalk address for the port. The default is no suggested address.

Note: An AppleTalk address consists of the network number followed by a node Id. For example, if the network number is 1234, and the node's Id is 56, the node's AppleTalk address would be 1234.56.

ROUTING PROTOCOL
Specifies what routing protocol the system should use with this remote device. Since Routine Table Maintenance Protocol (RTMP) periodically sends out routing updates, *RTMP* should be chosen only when the remote device is connected over the WAN links whose cost is not a major concern, such as dedicated links. The default value is *None.*

CONFIGURING THE APPLETALK PROTOCOL

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure for the AppleTalk protocol, or click *Add* to configure a new user. The *User* dialog appears.
3. Select *AppleTalk* on the *Protocols* tab.
4. *Enable* AppleTalk by clicking in the box.
5. Determine if the user is *Callable.*

   Note: A telephone number through which a CyberSWITCH can establish a connection must be configured before enabling the callable function. See *Configuring Telephone*.
6. Enter a *Network Number*, if necessary.
7. Enter a *Node ID*, if necessary.
8. Select a *Routing Protocol.*
9. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.
10. Click *Close.*

Note: An AppleTalk Routing Port must be defined on all CyberSWITCHES that each AppleTalk user can access. Refer to the *AppleTalk Routing Ports* section in the CyberSWITCH documentation for further information.

RESTRICTIONS

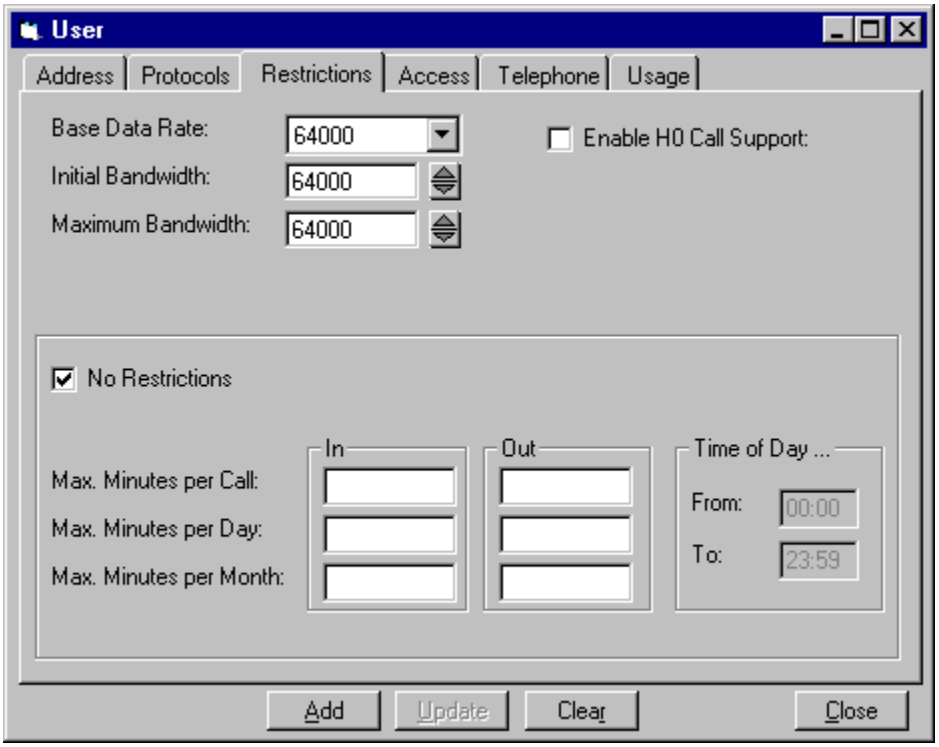
Data rates are required for all users. The base data rate value represents the data rate of one channel. This rate can be specified as either 56000 bps or 64000 bps. The initial data rate and the maximum data rate are used in combination with the base data rate. The initial data rate determines the number of calls that will be attempted when opening the first wide area connection. It provides a mechanism to request that a group of parallel connections be made rather than a single connection. For example, if the base data rate is set at 64000 bps, and the initial data rate is set at 256000 bps, the CyberSWITCH would attempt to make four (256000 / 64000 = 4) connections running in parallel. The maximum data rate determines the total number of connections that can be committed to a single logical connection. For example, if the base data rate is set at 64000 bps, and the maximum data rate is set at 512000 bps, the CyberSWITCH would allow a maximum of eight (512000 / 64000= 8) connections to be committed to a single logical connection.

The Call Restriction feature provides the ability to place limits on the toll costs of operating the SFVRA Connection Manager. Call Restriction consists of a variety of features that can restrict the number of switched calls made to remote sites, and also limit the amount of call minutes accumulated for remote site access.

Notes: When a condition occurs that triggers a call disconnection, a message will be written to the Problem Log, noting statistical information about the call, and stating "Time Restriction" as the failure type.

For example, if the network's total amount of connect time is estimated to be less than three hours per day, call restrictions could be set up to place a limit on the number of call minutes per day to 240. (Three hours would be 180 minutes; however, there may be some unusual days that go over a little, hence, 240 minutes.) If a newly installed application starts sending out packets on the LAN that causes remote connections to be made all the time, the system will terminate the call, and prevent any more calls from being made after 4 hours (240 minutes) of connect time to the remote site. Thus, the phone bill would be limited to just four hours of connection time.

Call Restrictions is disabled by default. If are enabling Call Restrictions, you must configure non-zero values for each parameter in order for calls to be accepted. In addition, the value for the maximum minutes per call cannot be greater than the maximum minutes per day, and the maximum minutes per day cannot be greater than the maximum minutes per month.



BASE DATA RATE

Only used for outbound calls. This value represents the data rate of one channel. The data rate can be specified as either 56,000 or 64,000 bps. A data rate must be defined for each remote device that will be dialed. The initial data rate and the maximum data rate configuration elements must also be configured for the Callable feature, and are used in combination with the base data rate. The default configuration for the base data rate is 64,000 bps.

INITIAL BANDWIDTH

Only used for outbound calls. The initial bandwidth determines the number of calls that will be attempted when opening the first wide area connection. This provides you with a mechanism to request that a group of parallel connections be made to a remote device rather than a single connection. This will allow data to begin to flow at greater rates without waiting for the Throughput Monitor to detect an overload condition. Calls will be made until an additional call would exceed the configured value. The value is configured as a number from 0 bps to 999,999,999 bps. You may configure any value in this range. For example, if you have configured the base data rate at 64 Kbps, and the initial bandwidth at 256,000, the system would attempt to initially use four calls (connections) running in parallel (256,000 / 64,000 = 4). The value need not be a multiple of the base data rate. The default configuration for the initial bandwidth is 64,000 bps.

MAXIMUM BANDWIDTH

The maximum data rate is used to limit the total number of channels that can be committed to a single logical connection. This sets an upper boundary for line and capacity utilization. This upper boundary allows you to keep one remote device from crowding out other users and using an unfair share of available resources. This parameter is enforced on inbound and outbound calls. The system will not accept or make a call when the added bandwidth will exceed the configured maximum. The value is configured as a number from 0 bps to 999,999,999 bps. You may configure

any value in this range. For example, if you have configured the base data rate at 64,000 bps, and the maximum data rate at 512,000 bps, the system would use a maximum of eight calls (connections) running in parallel to open up bandwidth (512,000 / 64,000 = 8). The value need not be a multiple of the base data rate. The default configuration for the maximum data rate is 128,000 bps.

ENABLE H0 CALL SUPPORT
If enabled, provides support for H0 calls operating at 384 Kbps. This provides one full 384 Kbps channel through the ISDN network and reduces the overhead associated with aggregating multiple channels. It is also almost always less expensive than the equivalent six 64 Kbps calls. Not all ISDN networks provide support for H0 calls. This is dependent upon the ISDN service provider as well as the switch manufacturer.

NO RESTRICTIONS
Defines the user to have no restriction on the time of day that calls are made, the length of any particular call, or the maximum minutes per day or month. No Restrictions is enabled as the default.

MAXIMUM MINUTES PER CALL
The maximum amount of time (in minutes) that a call is allowed to be active. The default value is 0 minutes. Statistics will be kept to track the total number of call minutes made per call. This statistic will be written to the statistics log every half minute. The current value of this statistic will be displayed on the Current Connections table. Existing calls that have surpassed the maximum minutes per call will be disconnected.

MAXIMUM MINUTES PER DAY
The limit of number of call minutes per day. The default value is 0 call minutes per day. Call minutes will be calculated periodically while calls are active (not when a call is disconnected). Statistics will be kept to track the total number of call minutes made per day. This statistic will be written to the statistics log every half minute. The current value of this statistic will be displayed on the Usage tab. Existing calls that have surpassed the maximum minutes per day will be disconnected, and no more calls from this user will be accepted until the next day, unless the administrator resets this user's restrictions.

MAXIMUM MINUTES PER MONTH
The maximum number of call minutes per month. The default value is 0 call minutes per month. Call minutes will be calculated periodically while calls are active (not when a call is disconnected). Statistics will be kept to track the total number of call minutes made per month. This statistic will be written to the statistics log every half minute. The current value of this statistic will be displayed on the Usage tab. Existing calls that have surpassed the maximum minutes per month will be disconnected and no more calls from this user will be accepted until the next month, unless the administrator resets this user's restrictions.

TIME OF DAY
The allowable hours for outbound calls (there are no time of day restrictions for inbound calls). Calls attempted outside of this time frame will be rejected. Calls that originated within this time frame, but extend outside of the limits will be disconnected. Selecting a "From" value of 00:00 and a "To" value of 00:00 allows the user access during any time of day.

CONFIGURING RESTRICTIONS

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

2. Select a user that which you want to configure restrictions, or click *Add* to configure a new user. The *User* dialog appears.

3. Select the *Restrictions* tab.

4. Select 56000 bps or 64000 bps for the *Base Data Rate*. 64000 bps is the default.

5. Determine the *Initial Bandwidth* and *Maximum Bandwidth*. These values do not have to be multiples of the Base Data Rate.

6. *H0 Call Support* can be enabled for users who need bandwidth to accomplish large file transfers or video conferencing. This feature is not cost effective for users who generate a smaller amount of network traffic.

7. Determine any time restrictions for the user. The default is no restrictions. Disable *No Restrictions* in order to configure time restrictions.

   Note: If *No Restrictions* is disabled, you must configure the non-zero values for each restriction parameter for a specific call direction before the user is allowed to connect.

8. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.

9. Click *Close*.

ACCESS

SFVRA Connection Manager performs device level security. Device level security is an authentication process between internetworking devices, in which authentication takes place automatically. Both bridges and routers support this form of security. An offnode authentication server can perform User level security as an optional feature. Configure device level security for each remote device. Group assignments and other features such as call back and compression are configured in this section.

AUTHENTICATION

DEVICE LEVEL AUTHENTICATION ON SFVRA-CONN

When a remote device calls a CyberSWITCH, the CyberSWITCH accepts the call. The authentication process begins by the user sending its authentication data to the CyberSWITCH. The CyberSWITCH passes this information on to SFVRA Connection Manager in an Authentication Request message. The SFVRA-CONN validates the information against its database, and sends an Authentication Reply to the CyberSWITCH indicating whether the user is valid or not. If the remote device is a valid user, the CyberSWITCH will negotiate connection parameters, such as the

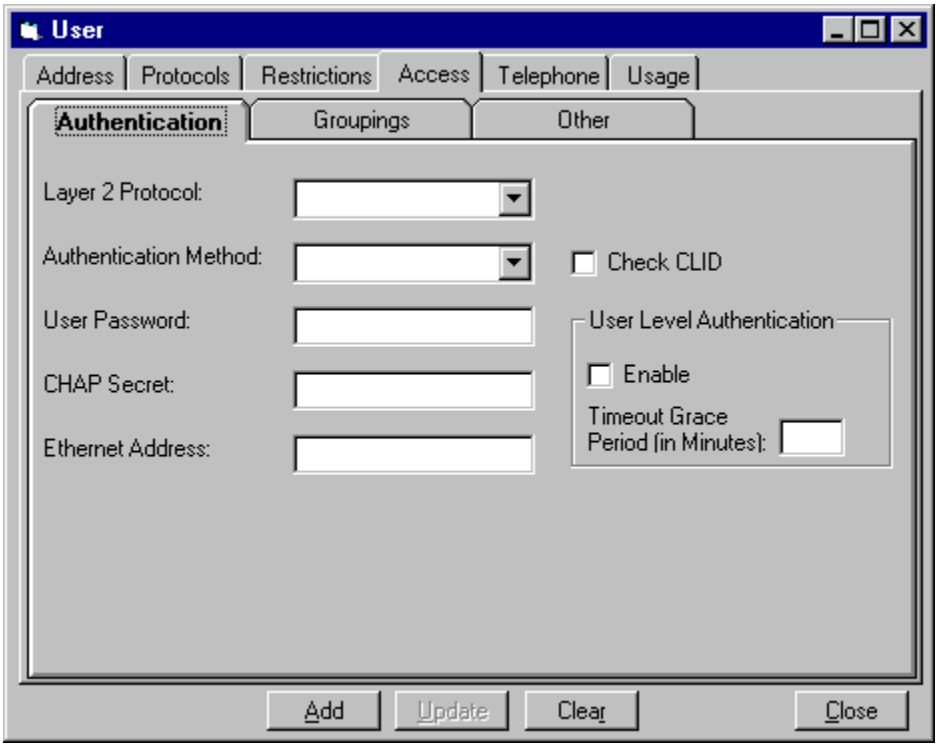
Layer 2 Protocol (PPP or CPP), with the remote device. Once this is negotiated, the CyberSWITCH sends a Connect Request to SFVRA-CONN. SFVRA Connection Manager checks time and bandwidth restrictions for the remote device and sends a Connect Reply back to the CyberSWITCH, indicating whether the call is acceptable. The CyberSWITCH then sends a Call Accept message to the remote device and a Connect Notify message to SFVRA-CONN, which then logs the call from the remote user and monitors the connection time.

OFFNODE USER LEVEL AUTHENTICATION WITH SFVRA-CONN DEVICE LEVEL AUTHENTICATION

This feature provides device level authentication by the SFVRA Connection Manager service while also requiring user level authentication from an off node authentication server, such as RADIUS, ACE, or TACACS. The user level authentication can be configured with a grace period. When a connection to the remote device completes user level authentication, the grace period starts. If a connection is re-established before the grace period expires, the user level authentication is not required.

The remote device is authenticated at the device level, as described in *Device Level Authentication on SFVRA-CONN*. During the device level authentication process, SFVRA-CONN checks the grace period, if the remote device is configured for user level authentication. If the grace period has not expired, SFVRA-CONN disables user authentication, and sends this information in the Authentication Reply message. If SFVRA-CONN accepts the call, and if the grace period has expired, the remote device must initiate user level security through a Telnet connection to the CyberSWITCH. The CyberSWITCH sends this information to the offnode authentication server. Upon successful user level authentication, the CyberSWITCH will begin the grace period by sending a message to SFVRA-CONN.

Note: Users must be on dial-up hosts or bridged PCs. Only bridging and IP are supported with User Level Authentication.



LAYER 2 PROTOCOL
The data-link protocol for a user. Select Combinet Proprietary Protocol (CPP) for Combinet users, or select Point to Point Protocol (PPP) for all other users.

AUTHENTICATION METHOD
For device level authentication methods, the choices are PAP, CHAP, CLID, CPP, NT, or none. If PAP or CHAP is chosen, then a password must be specified. If CPP is chosen, then an Ethernet address should be provided.

PAP PASSWORD SECURITY
PAP Security provides a method for the User to identify itself to the system using a 2-way handshake. If PAP Password Security is enabled, and a PAP Password has been configured for the User, the following holds true:

- After the initial connection is made, the remote device repeatedly sends the User Name and Password to the system. The system will look up the received User Name in the User List.
- If the User Name is not found, the call is disconnected.
- If the User Name is found the system will validate the password.
- If the password does not match, the call will be disconnected.
- If PAP Password Security is enabled, and a PAP Password has not been configured for the User, Password validation is not performed.

CHAP CHALLENGE SECURITY
An authentication phase between the remote device and the system begins with sending a CHAP challenge request to the remote device. The CHAP request contains a string of bytes known as the challenge value, which is changed on each challenge. Using the hash algorithm associated with CHAP, the remote user transforms the challenge value plus its secret into a response value. The

remote user sends this output of the hash function, along with its symbolic name, to the system in a CHAP response.

Within the User Records entry for each remote device that will be authenticated via CHAP, the system maintains the remote device's secret. The name in the remote device's CHAP response is used to locate the User Table entry, and consequently the secret used by the remote device. Using the same hash function, the system computes the expected response value for the challenge with that secret. If this matches the response value sent by the remote device, a successful authentication has occurred. The system can optionally be configured to repeat the CHAP challenge process periodically throughout the life of the connection. An invalid response to a CHAP challenge at any time is deemed a security violation, which causes a switched link to be released.

The above process applies to the system's authentication of the remote device. It is also possible that the remote device may wish to authenticate the system itself, a desire that is also negotiated during the LCP initialization of the link. Enabling CHAP via configuration also permits the system to agree to be authenticated via CHAP during LCP negotiation. In the same manner that each remote user has a name and secret, the system itself is configured with a system-wide name and secret that are used to respond to CHAP challenges.

Note: When both CHAP and PAP are available for a user, configure the user for CHAP authentication.

NT AUTHENTICATION

The SFVRA Connection Manager provides the ability to authenticate remote users on the local Windows NT server. The remote user must have an account established on the NT server in order to be authenticated. The process of authentication does not establish a connection between the remote user and the server. SFVRA-CONN merely uses the Windows NT security feature to verify the remote user password.

Note: PAP Password Security must be enabled on both the CyberSWITCH and the remote user.

USER PASSWORD

This password is used by PPP line protocol, for PAP authentication, or by the CPP line protocol as the bridge password. When used with PAP authentication, this is an unencrypted password value (a string of 1 to 12 ASCII characters) used as a security check when PAP Password Security is enabled. (PAP is an authentication protocol defined in RFC 1334 as part of the PPP protocol suite.) When used as a bridge password, the password is a secondary security check. This password is required when used for PAP authentication, but is optional for CPP authentication. At connection establishment time, the calling party sends an unencrypted User identifier and password combination over the WAN to the system. The system looks up the User Name based on the received User identifier and validates the password for that User. If the password received matches the password configured for the identified User, the call is accepted. Otherwise, the call is disconnected.

CHAP SECRET

This field is used by PPP line protocol, for CHAP authentication. This is a string of 1 to 17 ASCII characters that is used as a security check when CHAP Challenge Security is enabled. (CHAP is an authentication protocol defined in RFC 1334 as part of the PPP protocol suite.) CHAP is characterized by a highly secure challenge and response mechanism which is performed at connection setup and which can optionally be repeated throughout the existence of the connection. A shared CHAP Secret is configured for the devices at both ends of the connection. As opposed to a password, a CHAP Secret is not sent across the link, and therefore is not susceptible to

interception. Instead, a calculation is done on the packets transmitted between the two devices, and the results are compared to the shared CHAP Secret for validation. If the calculation's results do not match the expected results, the connection is terminated.

ETHERNET ADDRESS
This address is used for authentication purposes on connections made over the Combinet Proprietary Protocol (CCP). It is required if CPP is enabled as the authentication method. This is the MAC address of the remote bridge device. This value is passed to the system (in band) when a connection is established. The system will look up the incoming Bridge Ethernet Address in the User List. If the address is not included on the User List, the system will reject the incoming call. If the address is included on the User List, and the corresponding user entry is not configured with a password, the connection will be established. If the address is included on the User List, and the corresponding user entry is configured with a password, the system will validate the password before establishing the connection.

CALLING LINE ID SECURITY
Validates the Calling Line information received when an ISDN connection is made. The system will compare the incoming Calling Line ID with the value configured (if any) in the User List. If the numbers are identical the connection will be established. Otherwise, the system will reject the incoming call.

When the Calling Line ID security is enabled, entering a Calling Line ID for each remote user is optional. When two remote devices share the same line (a single point-multipoint ISDN line), they can also configure the same Calling Line IDs if they both also have some other type of authentication configured (for example, PAP, CHAP, NT Authentication, or CPP Authentication).

The following table illustrates the dependencies between other authentication methods and the Calling Line ID authentication:

PAP Authentication	*CHAP Authentication*	*NT Authentication*	*CPP Authentication*	*Calling Line ID Authentication*
Yes	No	No	No	Optional. Duplicates allowed for these Users.
No	Yes	No	No	Optional Duplicates allowed for these Users.
No	No	Yes	No	Optional Duplicates allowed for these Users.
No	No	No	Yes	Optional Duplicates allowed for these Users.
No	No	No	No	Required Duplicates not allowed.

Note: If a system is brought on line with a user that has a required Calling Line ID that is a duplicate of another user's Calling Line ID, and no other type of authentication is used, a warning message is logged at initialization. Every attempt to connect the user thereafter will result in an error message being logged and the call being rejected.

ENABLE USER LEVEL AUTHENTICATION
Indicates that the remote device requires user level authentication. SFVRA-CONN authenticates the remote device at the device level, and an offnode authentication server, such as RADIUS, ACE, or TACACS, preforms user level authentication.

TIMEOUT GRACE PERIOD
The grace period is the amount of time, in minutes, that the user will not be re-authenticated at the user level.

CONFIGURING AUTHENTICATION

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

2. Select a user that which you want to configure authentication, or click *Add* to configure a new user. The *User* dialog appears.

3. Select *Authentication* on the *Access* tab.

4. Select *PPP* or *CPP* as the *Layer 2 Protocol*.

5. Determine the *Authentication Method* for the user.

6. Enter a password or secret. Depending on which authentication method you choose, supply a password or secret for the following fields:
   - User Password — required for PAP, optional for CPP
   - CHAP Secret — required for CHAP and NT authentication
   - Ethernet Address — required for CPP

7. Enable *Check CLID* for additional security, if necessary.

8. Enable *User Level Authentication*, if necessary. Enter a grace period.

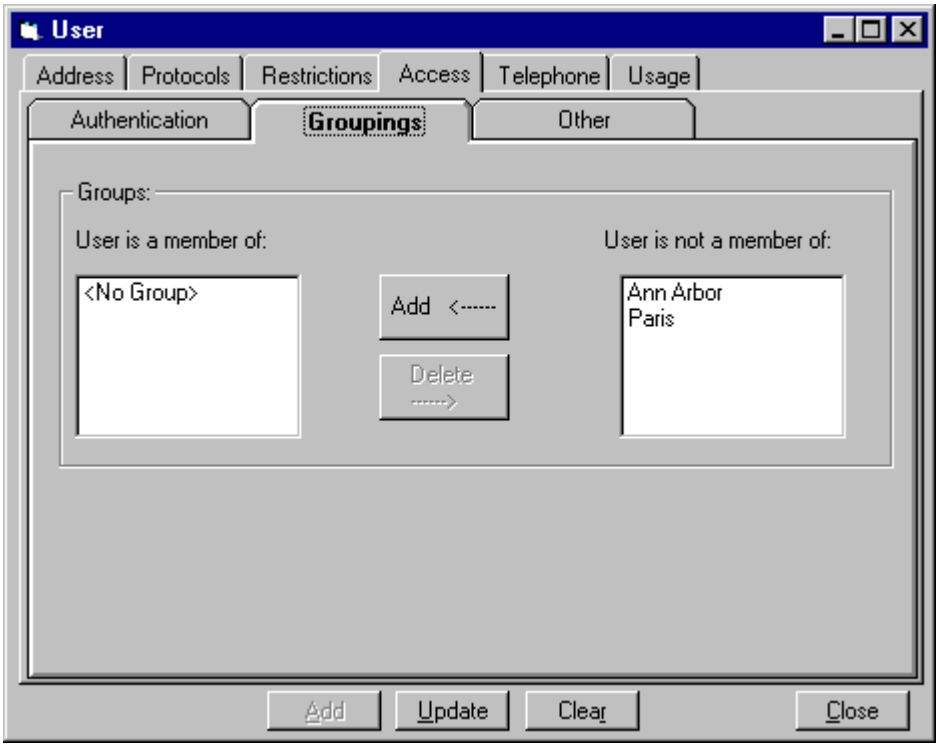
9. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.

10. Click *Close*.

GROUPING USERS

In order for Users to call the CyberSWITCH systems that have been assigned to a group, the user must be in the same group. Any CyberSWITCH that receives a call from a user that does not belong to the same group that the CyberSWITCH belongs will reject the call. By default, users belong to <No Group>. Users may be configured to belong to more than one group.



USER IS A MEMBER OF
A list of all groups that a user is a member. The user can connect to the Remote Access Switches in these groups.

USER IS NOT A MEMBER OF
A list of all groups that a user is not a member. The user cannot connect to the Remote Access Switches in these groups.

CONFIGURING GROUPING

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure groups. The *User* dialog appears.

   Note: The user must be added to the database before it can be assigned to a group.
3. Select *Groupings* on the *Access* tab.
4. Select a group(s) in the *User is not a member of* section and click *Add*. The group(s) shifts to the *User is a member of* section.
5. Click *Update* to write the new information for the user to the database.
6. Click *Close*.

OTHER

Other Access options allow for the configuration of compression and the Callback feature.

COMPRESSION

Compression allows a CyberSWITCH to compress outgoing data and decompress incoming data. This allows user devices on the WAN to initiate a connection to the system over the switched digital network and transmit and receive compressed data, thereby decreasing transmission time.

The system data compression capability allows the system to negotiate compression algorithms with a remote user. This compression can be done using some proprietary bridging protocols and also the PPP CCP protocol.

After successfully negotiating compression, data is compressed by a peer and transmitted to the system. The system decompresses the data, processes the addressing information contained in the user data, and transmits the data as required. The converse is also true, the system can receive data coming from a WAN or LAN and it compresses the data before transmitting it to a peer. The net effect is to increase interconnect bandwidth by decreasing transmission time. If negotiation for compression fails, data is transmitted uncompressed.

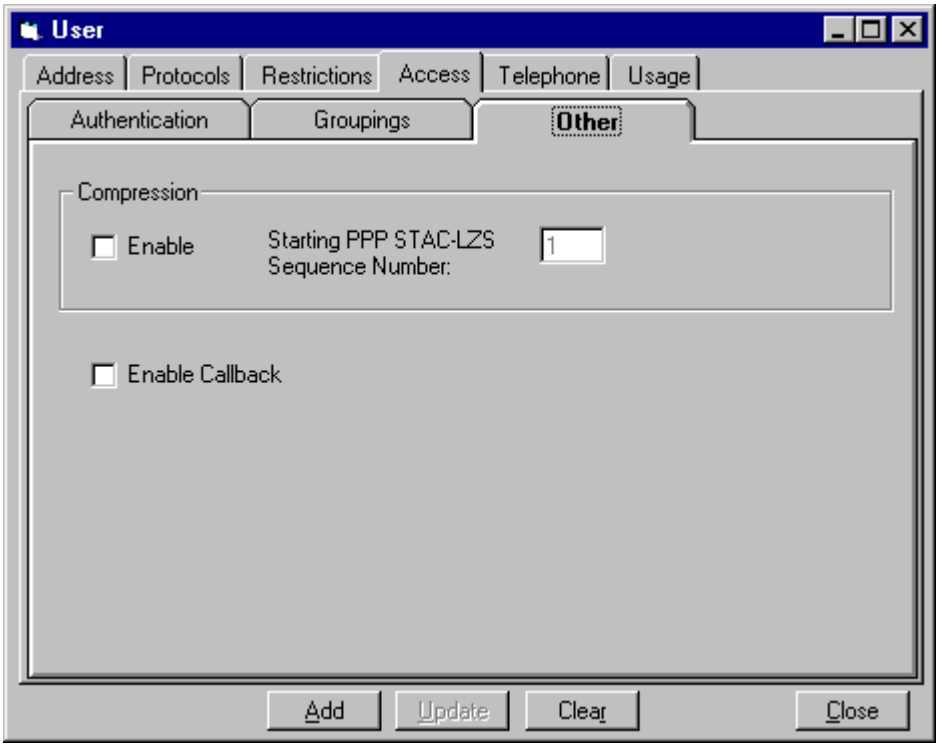
The compression software algorithm implemented is STAC-LZS. This algorithm is used in all of STAC's data compression products. This software version is fully compatible with STAC's data compression compressor chips including the multi-tasking features. STAC-LZS data compression is performed by replacing redundant strings in a data stream with shorter tokens. The STAC-LZS uses a compression history, or sliding window, as opposed to a structured dictionary. This allows greater flexibility and a greater number of possible string comparisons during compression process. The compression history automatically discards old information as new information is processed. Both the user device and system must perform compression using the STAC-LZS data compression algorithm. The peer and remote compression algorithms must be synchronized, this is accomplished by negotiating compression at channel connect time. Once this has been accomplished compressed data can be transmitted. If a transmission problem should ever occur the problem is detected and compression re-synchronized by the execution of a pre-defined protocol.

CALLBACK

In order to maximize security and centralized billing, calls can be required to be made from the central site to the remote site. This feature implements call back. In this process, the remote device calls in to the central site and is authenticated. SFVRA-CONN will verify that the user satisfies the configured call restriction, bandwidth and group requirements. If the user is validated, SFVRA-CONN will instruct the CyberSWITCH to disconnect the call. The "CyberSWITCH Callback" message will be logged as the reason for disconnection. The CyberSWITCH will then be instructed to reconnect to the user, based on the load leveling feature, at which time the user is authenticated again. The load leveling feature distributes outgoing Callback calls evenly among CyberSWITCHES within a CyberSWITCH - User Group. If the user does not have any current calls, SFVRA-CONN will examine all CyberSWITCH systems within the same group as the user. If a

CyberSWITCH is found which has at least two more free channels than the CyberSWITCH that received the call, SFVRA-CONN instructs a selected CyberSWITCH to re-establish a connection to this user.

Note: In order for the Callback feature to work properly, the user must be properly configured for Dial Out, and call restrictions must be disabled, or non-zero values must be configured for outgoing calls.



ENABLE
Select this option if this user is to negotiate compression during WAN communication. Combinet Compression is used if the "Layer 2 Protocol" is CPP, standard compression is used if the PPP has been selected. This feature is optional.

STARTING PPP STAC-LZS NUMBER
Default value is 1. When using PPP Compression with the STAC-LZS protocol, a sequence-numbering scheme can be used whose initial value is required to be 1 by the protocol specification. Some devices from other vendors do not start with 1. This results in a resynchronization sequence on the first frame that is exchanged. When the user device fully supports the CCP protocol's Reset mechanism, this will only result in the minor inconvenience of a lost frame at the beginning of a session. However, if such a device's resynchronization mechanism is to completely renegotiate CCP, this sequence will repeat infinitely.

This option provides an escape mechanism to allow interworking with such devices by modifying the initial PPP STAC sequence number.

The Starting PPP STAC Sequence Number is maintained for each user. The value that appears on this configuration screen provides the default value for the per-user value. When you add a new

user to the local user table, that user's starting sequence number option will be assigned the value that appears on this screen. You can then change this for each individual user. Or, if the user is authenticated via an off node server that does not deliver a value for this configuration item, the user will be given its starting sequence number from the value on this menu.

As its name implies, this option only applies to connections that utilize the PPP protocol with STAC-LZS compression and sequence numbers checking.

Note: The SFVRA-CONN does not support individual link compression when PPP Multilink is negotiated to aggregate multiple links. Multiple links to a single destination will be treated as a single high capacity link as far as PPP compression is concerned. One history will be kept for the group of links, and packets will be compressed before they are fragmented for transmission across the multiple links.

ENABLE CALLBACK
Indicates that a CyberSWITCH that receives a call from this user should disconnect and re-establish the connection. A CyberSWITCH within the same group that makes the returning call will have at least two more free channels than the CyberSWITCH receiving the incoming call, if applicable. Users must have a telephone number configured in order to enable this feature.

CONFIGURING OTHER FEATURES

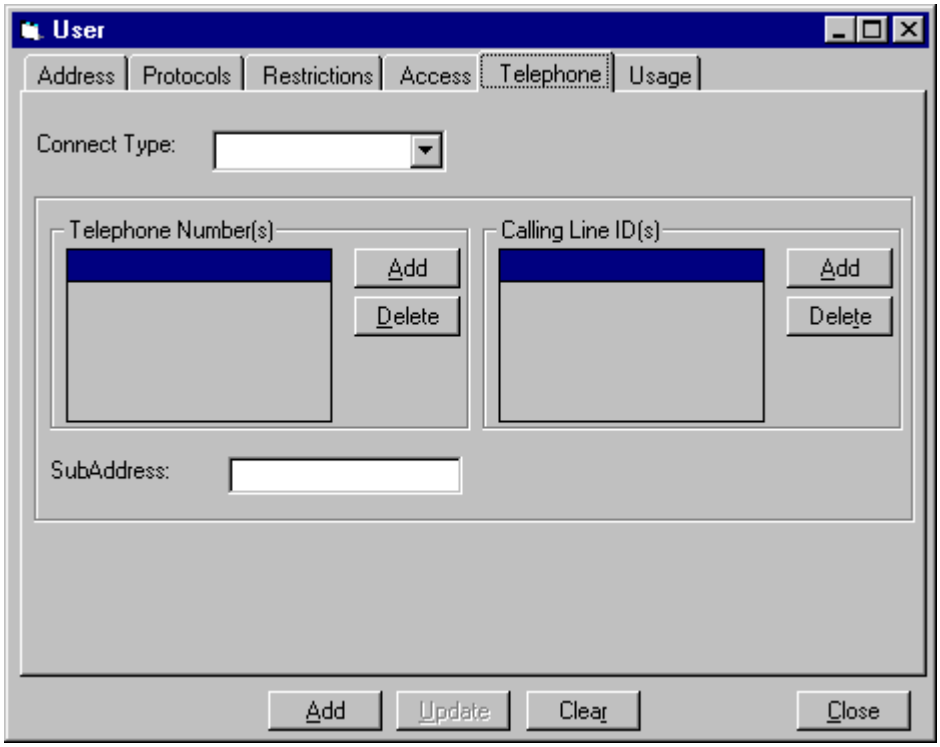
1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to configure other features, or click *Add* to configure a new user. The *User* dialog appears.
3. Select *Other* on the *Access* tab.
4. *Enable* compression, if necessary, and accept the default sequence number.
5. Enable *Callback*, if necessary.
6. Click *Update* to write the new information for the user to the database, or click *Add* to create the newly configured user.

   Note: If you are adding a new user to the database, a *User Name* must be defined on the *Address* tab.
7. Click *Close*.

TELEPHONE

If the Callable feature is enabled for a user, the CyberSWITCH systems will need to know how to reach the user. This section defines the connection type that the CyberSWITCH systems need to use and the telephone number(s) necessary to establish a connection.

If the Check CLID feature is enabled for a user, CLID's need to be defined. CLID's are unavailable for Digital Modem users.



CONNECT TYPE

The type of connection that is to be made when the Remote Access Switch attempts to connect to the user. This feature dictates what connection type the CyberSWITCH systems are to use to reach a user. This option only specifies outbound connection types. Available connection types are:

- ISDN
- Dedicated
- Digital Modem

TELEPHONE NUMBER(S)

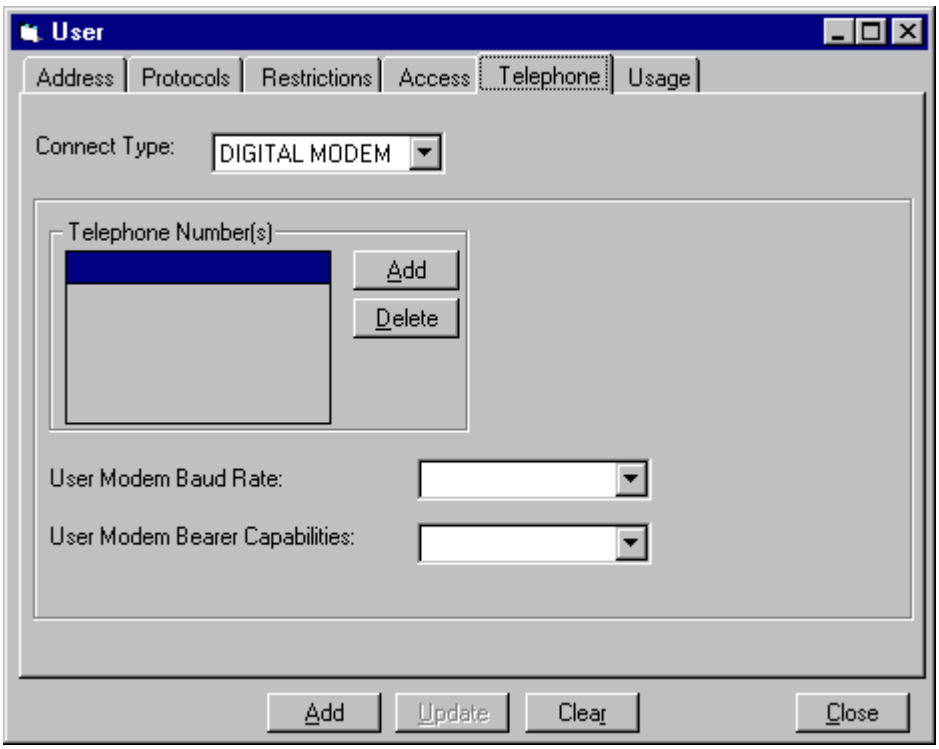
This configuration element is required when the Callable feature is used. The callable capability allows the SFVRA-CONN to initiate connections to PPP devices located at remote sites. A phone number must be defined for each remote device that will be dialed. This number includes any prefix digits, area codes, or extensions required to dial the destination device. It is possible to specify eight phone numbers for the remote device.

The system dynamically controls the bandwidth in use between the system and other devices. This is accomplished by establishing and disconnecting up to 8 calls to a single remote site over the digital network. The system monitors the connections for utilization and will add and remove connections based on the user configurable parameters described above (base data rate, initial data rate, and maximum data rate).

CALLING LINE IDENTIFIER (CLID)
Applicable to ISDN connections only, and only when the Check CLID option is enabled. You can specify eight CLIDs for each user entry. Each CLID for a given user must be unique. This is the telephone number of the calling party that is connecting to the system. In some areas this information is passed to the system on the ISDN incoming connection message. The system will compare the incoming CLID with the value configured in the User List. If the numbers are identical the connection will be established. Otherwise, the system will reject the incoming call. This identifier must be identical to the number received on the ISDN connection.

When two remote devices share the same line (a single point-multipoint ISDN line), they can also configure the same CLIDs if they both also have some other type of authentication configured (for example, PAP, CHAP, or Bridge MAC Address Authentication).

SUBADDRESS
The SubAddress is used by a CyberSWITCH when it attempts to make a connection to a user. A SubAddress allows the user to share a telephone number with other devices and yet still recognize calls destined for it.



USER MODEM BAUD RATE
The baud rate at which data will be transmitted. The only selection at this time is *Auto*. Auto means the device will negotiate the baud rate automatically, with user intervention.

USER MODEM BEARER CAPABILITIES
The frame type that is used to encapsulate the digitized analog modem signals. Choices are *Speech* or *3.1 kHz Audio*.

CONFIGURING TELEPHONE

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

2. Select a user that which you want to configure dial out, or click *Add* to configure a new user. The *User* dialog appears.

3. Select the *Telephone* tab.

4. Select *ISDN*, *Dedicated*, or *Digital Modem* as the *Connect Type*.

   Note: The user must be added to the database before a telephone number or a calling line ID can be configured.

5. Configure a Telephone Number(s). Click *Add* in the Telephone Number section, enter a number, and click *OK*.

6. Configure a CLID(s), if necessary. Click *Add* in the Calling Line ID section, enter a CLID, and click *OK*. Calling Line IDs are available only for ISDN and Dedicated connect types.

7. Enter a *SubAddress*. SubAddress is available only for ISDN and Dedicated connect types.

8. Accept the default *Baud Rate*. Currently, Auto is the only Baud Rate supported. The Baud Rate is only available for Digital Modem.

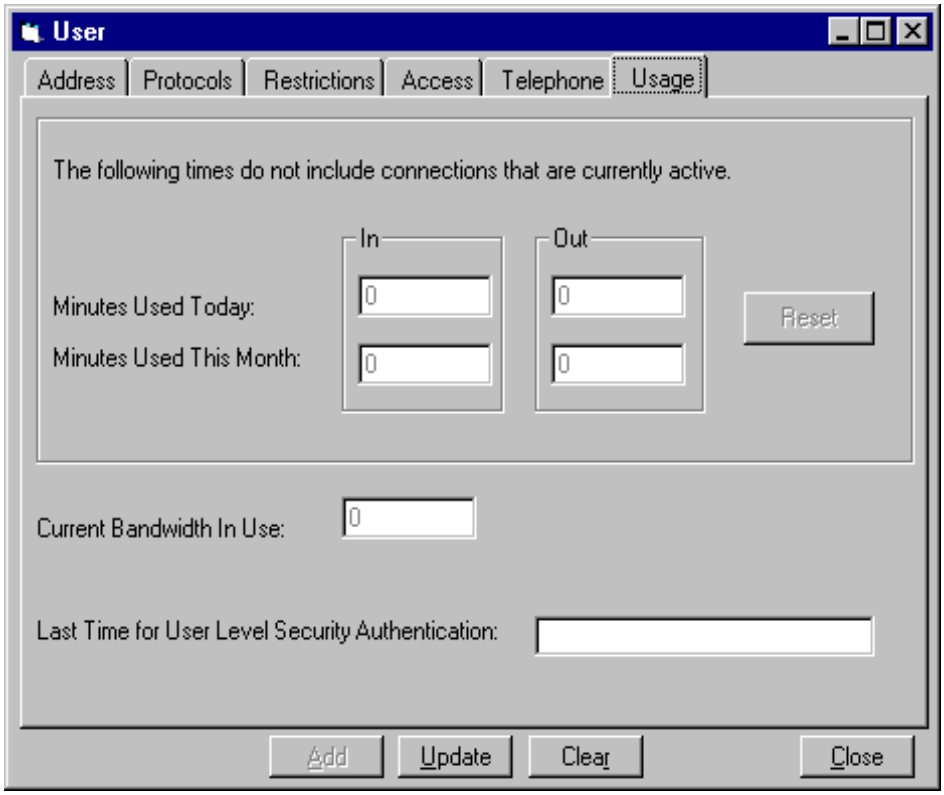
9. Select a *Bearer Capability*. The Bearer Capability is only available for Digital Modem.

10. Click *Update* to write the new information for the user to the database.

11. Click *Close*.

USAGE

The Usage window monitors the accumulated connection time for a specific user. The connection time displayed does not include time accrued by any current connections, nor is it updated dynamically if a connection is closed while viewing this information.



MINUTES USED TODAY

Displays the time, in minutes, that this user has been connected to a CyberSWITCH today through an inbound or an outbound connection.

MINUTES USED THIS MONTH

Displays the time, in minutes, that this user has been connected to a CyberSWITCH this month through an inbound or an outbound connection.

CURRENT BANDWIDTH IN USE

Displays the current bandwidth in use for this user's present connection.

LAST TIME FOR USER LEVEL SECURITY AUTHENTICATION

Displays the last time that this user was authenticated at the user level. This information can be compared with the grace period to determine if the user will be authenticated again at the user level.

RESET

This button resets the connection restrictions to zero for this user for the current month. This button is unavailable if the user has not made any connections this month.

VIEWING AND RESETTING CALL USAGE

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.
2. Select a user that which you want to view and/or reset the monthly call restrictions. The *User* dialog appears.
3. Select on the *Usage* tab.
4. Click *Reset* to reset the minutes used today and this month to zero for this user, if necessary.
5. Click *Update* to write the new information for the user to the database.
6. Click *Close*.

CONFIGURING CYBERSWITCH - USER GROUPS

OVERVIEW

Groups of CyberSWITCH systems and users may be configured, in order to allow the SFVRA Connection Manager to better manage its devices. By grouping the CyberSWITCH systems and users, you can not only limit which users can call which CyberSWITCH, but you can manage which CyberSWITCH can call which users. This can reduce costs by eliminating calls from CyberSWITCH systems that may not have the cheapest direct connection to certain users.

A CyberSWITCH may only belong to one group. However, users may be a part of many groups. There is no limit to the number of CyberSWITCH systems or users in a group. CyberSWITCH systems and users that do not belong to any group are classified by SFVRA-CONN into a group with no name, designated by <No Group>.

Only devices of the same group may call each other. If a user attempts a connection to a Remote Access Switch not in its group, SFVRA-CONN will reject the call and enter in the database Problem Log table an entry with the Failure Type "Connect Failed" and the Reason "User not part of this group." For outgoing calls, SFVRA-CONN determines to which user the call is to be made and then searches the database for a Remote Access Switch in the same group. If there is no Remote Access Switch in the group, SFVRA-CONN will not make the call and enter in the database Problem Log table an entry with the Failure Type "Connect Failed" and Reason "No Remote Access Switch for this users group."

Note: Configuring a user in multiple groups can adversely affect the behavior of the network. Users that are remote hosts and are dynamically assigned an IP address should not have a problem. SFVRA-CONN will not check for the following situations where problems may occur.

1. A user that is a RLAN attached bridge with a permanently assigned IP address. This address would only be relevant to a single-site CyberSWITCH.

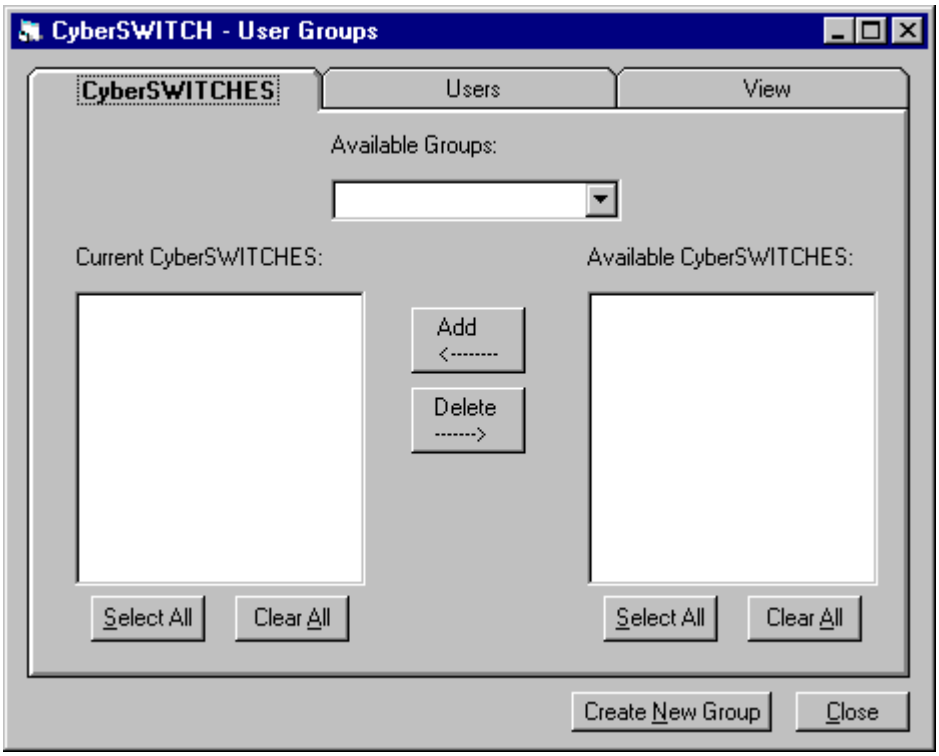
2. A user that has static routes configured and these routes are being advertised by multiple systems without the SFVRA RIP service being used.

3. IP users with call out enabled will have their routes advertised by multiple groups. Multiple CyberSWITCH systems may try to reach the user at the same time.

Groups may be assigned individually to devices within the configuration utilities of the SFVRA Connection Manager for the CyberSWITCH or the user. Refer to *CyberSWITCH Properties* or *Grouping Users* for more information. Groups may also be assigned collectively on the CyberSWITCH - User Groups configuration utility, as described in the following sections.

CYBERSWITCHES

A CyberSWITCH may be assigned to a group individually or by selecting many CyberSWITCHES. The Clear All button deselects currently selected CyberSWITCHES.



AVAILABLE GROUPS
A list all groups currently configured in the SQL database.

CURRENT CYBERSWITCHES
A list all CyberSWITCHES currently configured to be a part of this group.

AVAILABLE CYBERSWITCHES
A list of all CyberSWITCHES currently available to be configured into a group. Devices listed here are part of <No Group>.

GROUPING CYBERSWITCHES

1. On the *Functions* menu, select *CyberSWITCH - User Grouping*, or click on the toolbar. The *CyberSWITCH - User Groups* dialog appears.

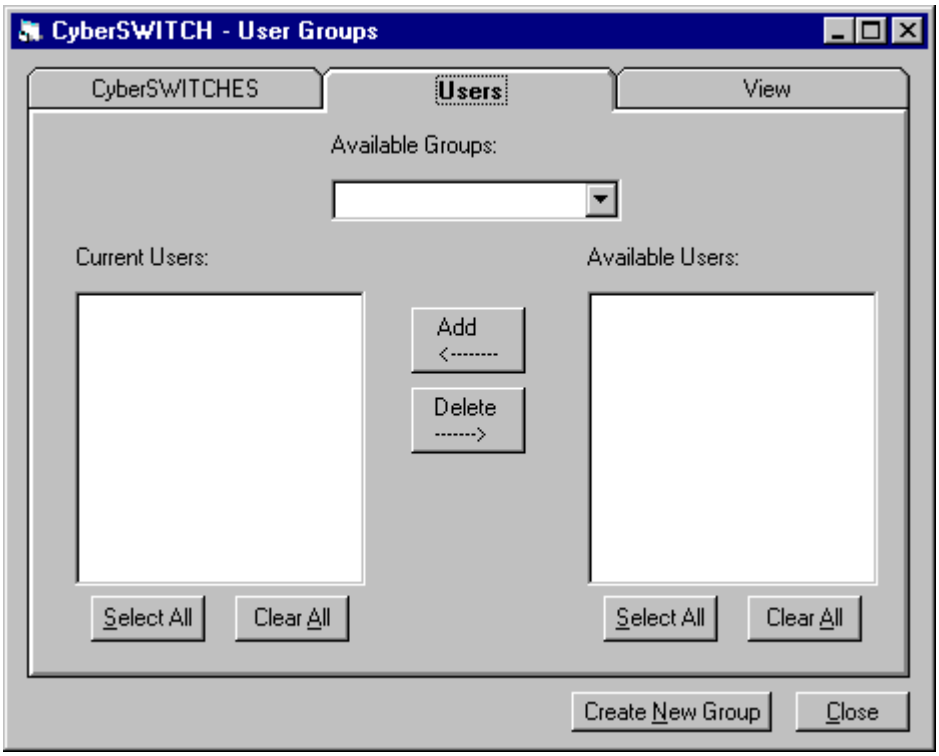
2. On the *CyberSWITCHES* tab, select an available group from the pull-down menu. See *Creating a New Group* to configure a new group.

3. Select CyberSWITCH from the *Available* list and click *Add* to assign the device to the specified group. The CyberSWITCH shifts to the *Current* list.

4. Click *Close*.

USERS

A user may be assigned to a group individually or by selecting many users. The Clear All button deselects currently selected users.



AVAILABLE GROUPS
A list all groups currently configured.

CURRENT USERS
A list all Users currently configured to be a part of this group.

AVAILABLE USERS
A list of all Users currently available to be configured into a group. Devices listed here are part of <No Group>.

GROUPING USERS

1. On the *Functions* menu, select *CyberSWITCH - User Grouping*, or click on the toolbar. The *CyberSWITCH - User Groups* dialog appears.

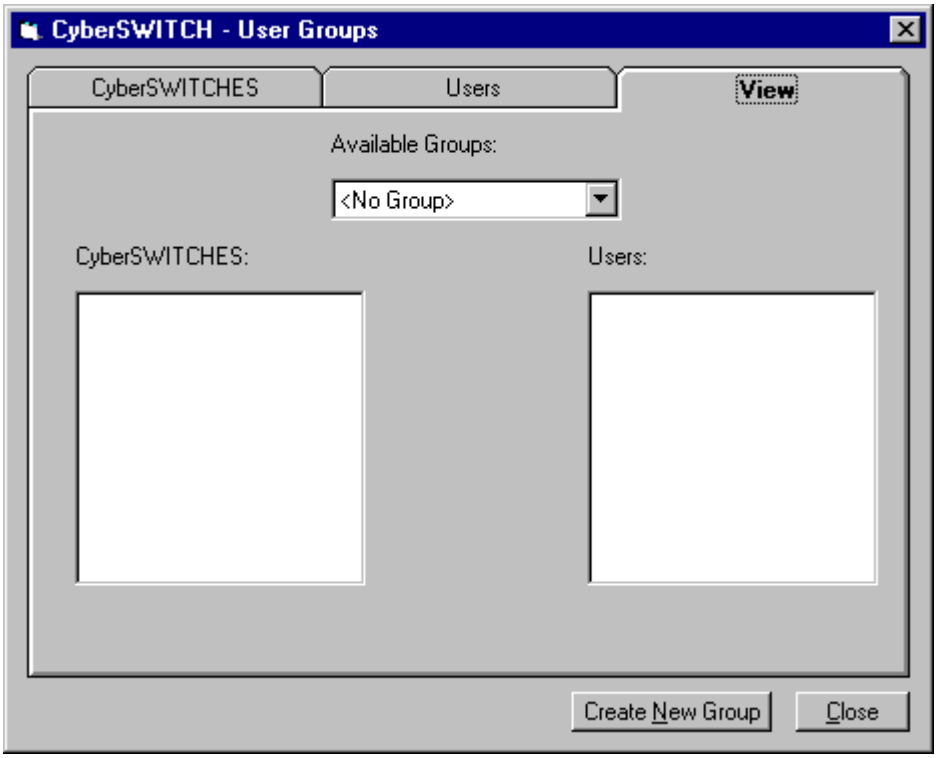
2. On the *Users* tab, select an available group from the pull-down menu. See *Creating a New Group* to configure a new group.

3. Select user from the *Available* list and click *Add* to assign the device to the specified group. The user shifts to the *Current* list.

4. Click *Close*.

VIEW

On the View tab of this utility, both CyberSWITCHES and users are displayed together in their group. This allows you to view each group as a whole. Devices that do not belong to any group are listed in the <*No Group*> category.



CYBERSWITCHES
A list of all CyberSWITCHES that have been assigned to a specified group.

USERS
A list of all users that have been assigned to a specified group.

VIEWING GROUPS

1. On the *Functions* menu, select *CyberSWITCH - User Grouping*, or click on the toolbar. The *CyberSWITCH - User Groups* dialog appears.

2. On the *View* tab, select an available group from the pull-down menu. All CyberSWITCHES and users configured for the selected group appears below in the two tables. See *Creating a New Group* to configure a new group.

3. Click *Close*.

CREATING A NEW GROUP

1. On the *Tables* menu, select *CyberSWITCH - User Grouping*, or from the CyberSWITCH -User Groups configuration interface click *Create New Group*. The *Table Maintenance* dialog appears.

2. Click *Add*.

3. Enter the group name and click *OK*.

4. Click *Close*.

CONFIGURING NETWORK PROXIES

OVERVIEW

Routing Information Protocol (RIP) is a protocol used to exchange routing information among IP devices. The Remote Access Switches use RIP to automate the maintenance of routing tables on IP devices and relieves the administrator from keeping the routing tables up to date manually. RIP determines the shortest path between two points on a network in terms of the number of "hops".

Proxy Address Resolution Protocol (ARP) is a technique in which a router, SFVRA Connection Manager in this case, answers ARP requests intended for any of the remote devices in the database by supplying its own physical address. By pretending to be other machines, SFVRA-CONN accepts the responsibility for forwarding packets. The purpose of proxy ARP is to allow a site to use a single IP network address with multiple physical networks.

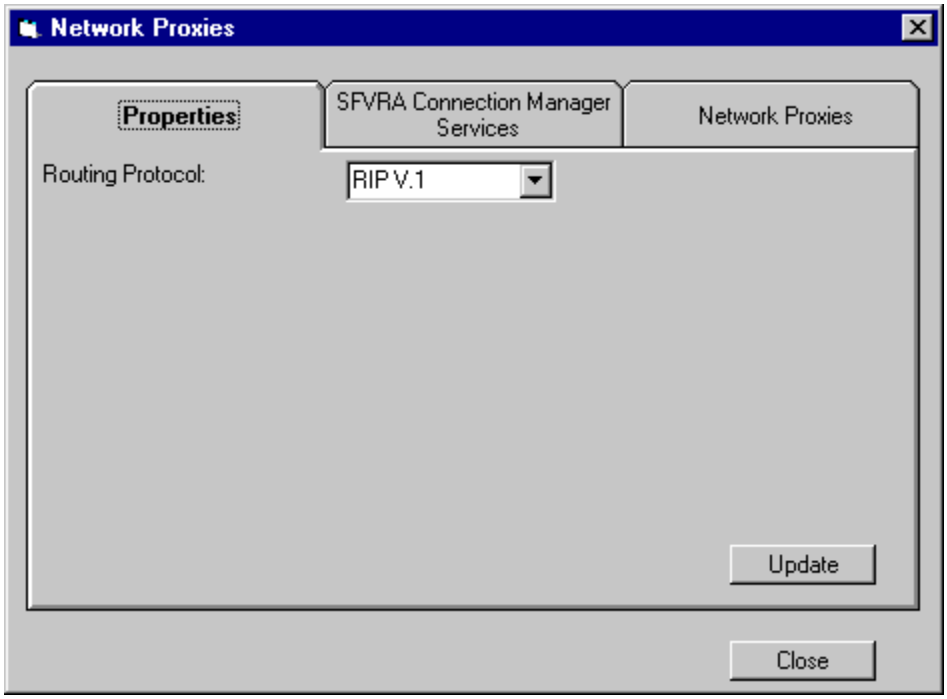
In order for these proxy services to interact with the SFVRA Service, the location of the service must be defined.

PROPERTIES

RIP v.1 broadcasts the network and metric. Using RIP v.1 requires that remote users have the same subnet. RIP v.2 broadcasts network, metric, mask and next hop. RIP v.2 is more flexible, but fewer systems support this version. All systems must support a common routing protocol.

Note: IP RIP v1 (IP RIP Version 1) supports broadcasts.
IP RIP v2 (IP RIP Version 2) supports multicasts.

SFVRA Connection Manager advertises the static routes of users who are allowed to be called so other devices will know how to call these users. However, when a remote user is connected to a CyberSWITCH, that CyberSWITCH also broadcasts the user's static routes. In order to resolve this double broadcast, SFVRA-CONN broadcasts a metric value of 16 for all users that have a current connection. Therefore the SFVRA-CONN's broadcasted routes appear "farther" than the routes broadcasted by the CyberSWITCH and then other devices use the current connection. When the user disconnects from the CyberSWITCH, the static routes are removed from the CyberSWITCH'S broadcast, and SFVRA-CONN's broadcast for that user returns to its original value.



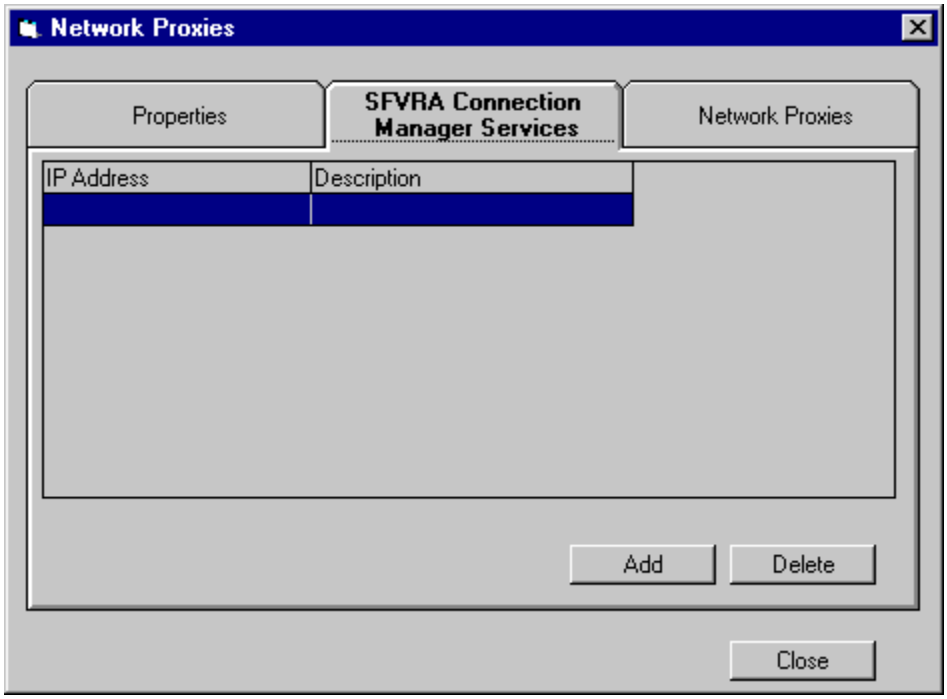
ROUTING PROTOCOL
Select the dynamic routing protocol for the SFVRA-CONN to implement. Currently supported protocols are RIP version 1 or RIP version 2.

CONFIGURING ROUTING PROPERTIES

1. On the *Functions* menu select *Network Proxies*, or click on the toolbar. The *Network Proxies* dialog appears.
2. Select the *Properties* tab.
3. Select desired version of RIP.
4. Click *Update* to write the new information to the SQL database.
5. Click *Close*.

SFVRA SERVICES

The SFVRA Service performs the remote user authentication and connection management functions. This service uses a standard ODBC connection to the SQL Database, whether the service resides on the same machine as the database or not. The IP address of each service must be configured, even if the service is on the same machine as the database, so that each RIP Service and each Proxy ARP Service can receive information about current connections with the Remote Access Switches.



IP ADDRESS
The IP Address used by the Network Proxies to connect to the SFVRA Service.

DESCRIPTION
The Description is an optional field that describes the SFVRA Service. For example, you may wish to set this to the computer name or location where the SFVRA Service is running.

CONFIGURING SFVRA SERVICES

1. On the *Functions* menu select *Network Proxies*, or click on the toolbar. The *Network Proxies* dialog appears

2. Select the *SFVRA Services* tab.

3. Click *Add* to configure a new SFVRA Service in the database.

4. Enter the *IP Address* that a RIP Service or Proxy ARP Service can use to connect to the SFVRA Service.

5. Enter a *Description*, if necessary.

6. Click *OK* to write the new information to the SQL database.

7. Click *Close*.

NETWORK PROXIES

The RIP service operates by advertising itself as a path to reach one or more remote subnets. If the RIP service data is destined for a remote subnet, the RIP service forwards the connection information to the SFVRA service. The SFVRA service will initiate a call to the remote subnet through a local CyberSWITCH. The CyberSWITCH then advertises itself as the path to the remote subnet. This procedure operates most efficiently when the RIP service resides on the same IP subnet as the CyberSWITCH that eventually makes the outgoing call, because local routers do not have to update their routing tables when a call is made. If the CyberSWITCHES are located on separate subnets, system performance is adversely affected when the RIP service only resides on the same machine as the SFVRA service.

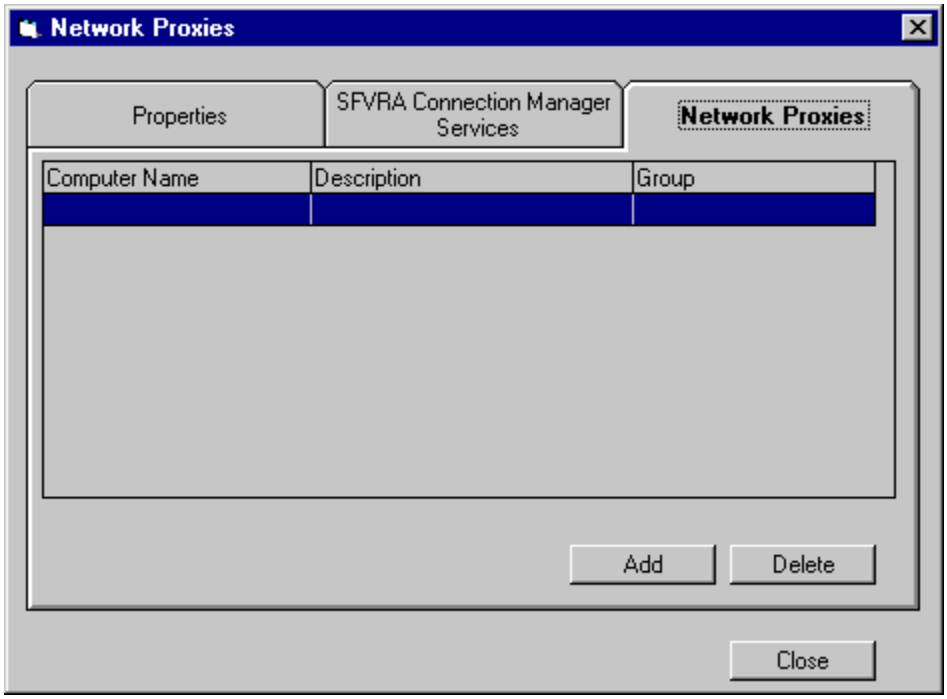
Distributed RIP services allows multiple RIP services to be located on the separate subnets. Each service only advertises for the CyberSWITCHES on its local subnet. Each RIP service can be configured to belong to one or more CyberSWITCH - User Groups. Since the services advertise for remote devices, assigning a RIP Service to a group(s) prevents multiple RIP Services from advertising for the same remote device.

The Proxy ARP Service will receive all ARP requests on the network. For each ARP request, the service will check the IP addresses and the static routes of all connected devices, and check the IP pool addresses currently in use for a match with the target IP address. If a match is found, a proxy ARP reply is sent using the MAC address of the connecting CyberSWITCH as the sender MAC address. If a match is not found, the service will check the IP addresses and static routes of all callable remote devices for a match with the target IP address. If a match is found, an ARP reply is sent using the MAC address of the local machine as the sender MAC address. This will cause any subsequent IP packets destined for the target IP address to be sent to the Proxy ARP Service.

A similar procedure is used for receiving IP packets as well. Each IP packet received, the service will check the IP addresses and static routes of all connected remote devices, and check the IP pool addresses currently in use for a match with the target IP address. If a match is found, the packet is discarded. If a match is not found, the service checks the IP addresses and static routes of all callable remote devices for a match with the target IP address. If a match is found, a request is sent to the SFVRA Service to establish a connection to the remote device. The IP packet is then placed into a list of pending IP packets. When a connection to the remote device is established, the SFVRA Service notifies the Proxy ARP Service. If the connection is not established within 15 seconds the packet is discarded.

The SFVRA Service sends notification messages to the Proxy ARP Service whenever connections are established or terminated. When the Proxy ARP Service receives a connection notification message, it marks the remote device as connected. It then checks the destination IP addresses in the list of pending IP packets for a match with the remote device's static routes or IP address. If a match is found, the Proxy ARP Service broadcasts a gratuitous ARP for the destination IP address with the CyberSWITCH'S MAC address as the sender MAC address. This will cause all local devices to update their ARP cache entry for this IP address, if they have such an entry.

The Proxy ARP Service can be configured to belong to one or more groups.



COMPUTER NAME
The Computer Name for the Windows NT system on which the RIP Service or Proxy ARP Service runs. This may be found on the Windows NT system by selecting Network from the Control Panel.

DESCRIPTION
The Description is an optional field that describes the RIP Service or the Proxy ARP Service. For example, you may wish to set this to the location where the RIP Service or Proxy ARP Service is running.

GROUP
The group for which the RIP Service or Proxy ARP Service will advertise routes.

Note: Multiple groups may be assigned to one Network Proxy, however, each group must be configured with the Network Proxy as a separate entry.

CONFIGURING NETWORK PROXIES

1. On the *Functions* menu select *Network Proxies*, or click on the toolbar. The *Network Proxies* dialog appears.
2. Select the *Network Proxies* tab.
3. Click *Add* to configure a new RIP Service or Proxy ARP Service in the database.
4. Enter the *Computer Name* of the system that runs the Network Proxy.
5. Enter a *Description*, if necessary.
6. Select a *Group* for which the Network Proxy will advertise routes.
7. Click *OK* to write the new information to the SQL database.
8. Click *Close*.

MONITORING CONNECTIONS

OVERVIEW

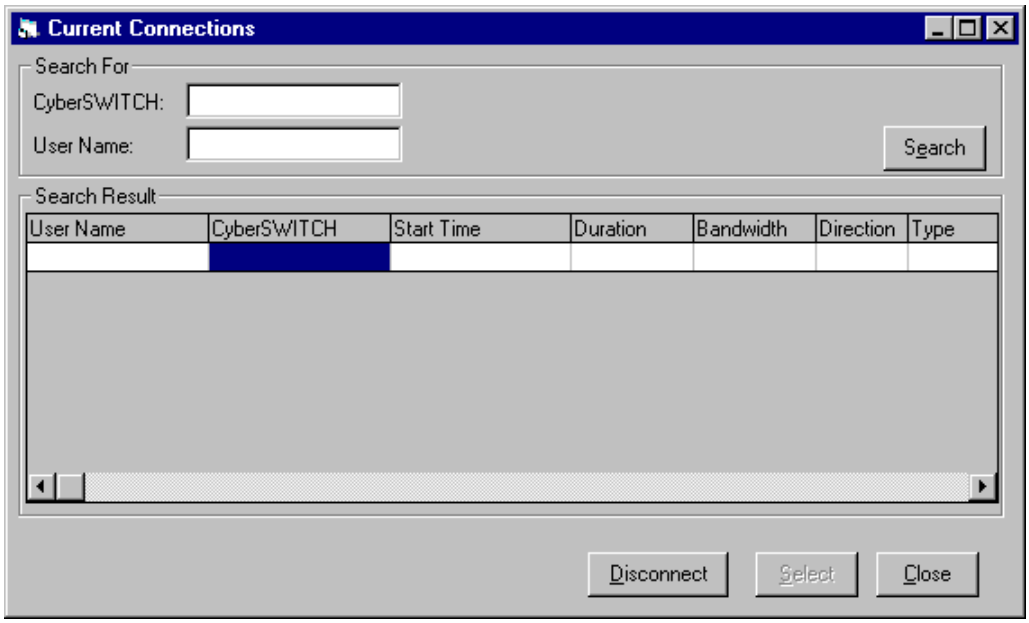
The SFVRA Connection Manager provides you with the ability to monitor all calls that are currently connected, those that were previously connected, and any problems that might have occurred with a connection.

- Current connections
- Past connections
- Problems with connections
- Creating reports on connections
- Database Information

CURRENT CONNECTIONS

The present connection log lists current connections chronologically. Data included in this list are the user name, the CyberSWITCH name, the start time of the connection, the duration of the connection, the current bandwidth, the direction of the call, the type of service being used, and the status, whether the call is active or unknown. The unknown state is entered for any connection with the SFVRA-CONN that was lost. If the connection is re-established, then "Unknown" will be changed to "Active". If the connection does not get re-established, then the listing is moved from the Current Connections table to the Connect History table. These statistics can also be viewed on the basis of each call that makes up a connection. The call display also lists the calling number, the called number, and a forwarding number if the called number is unavailable. The connections listed can be specific to a user, to a CyberSWITCH, to any combination of the two, or all user and CyberSWITCH systems.

Note: All references to time are based on the internal clock of the machine on which the database resides.



SEARCH

This button searches the SQL Database for the current connections based on the parameters that you define. You can search for a specific user or a specific Remote Access Switch or both. Leaving a search field blank indicates a search for all in that category.

CURRENT CALL AND CONNECTION TABLES

User Name
The remote user which the Remote Access Switch is connected.

CyberSWITCH Name
The Remote Access Switch which the user is connected.

Start Time
The time that this connection was established.

Duration
The current duration of this connection. This table is not updated dynamically, therefore the duration reflects the time since the connection was established until the Search button was pressed.

Current Bandwidth
The current bits per second established between the user and the Remote Access Switch.

Direction
The direction in which the connection was first established.

- DED stands for a dedicated connection.
- IN stands for a call from the user in to the Remote Access Switch.
- OUT stands for a call from the Remote Access Switch out to the user.

Type
The type of connection currently established. Types include:
- ISDN
- Dedicated
- Digital Modem

Status
The current status of the connection.
- Active means that the connection is currently in place.
- Unknown means the connection is in an unknown state. The unknown state is entered for any connection that was Active when the TCP connection between the Remote Access Switch and the SFVRA-CONN was lost.

Calling Number
The telephone number of the device that initiated the call.

Called Number
The telephone number of the device that was called.

Forwarding
The telephone number that can be used to access the device that was called if the called number is unavailable.

DISCONNECT
This button disconnects the connection between the currently selected user and CyberSWITCH.

VIEWING CURRENT CONNECTIONS

1. On the *Functions* menu, select *Current Connections*, or click on the toolbar. The *Current Connections* dialog appears.

2. To search enter a User Name, a CyberSWITCH name, or both and click *Search*.

   Note: Leaving a search field blank indicates a search for all in that category.

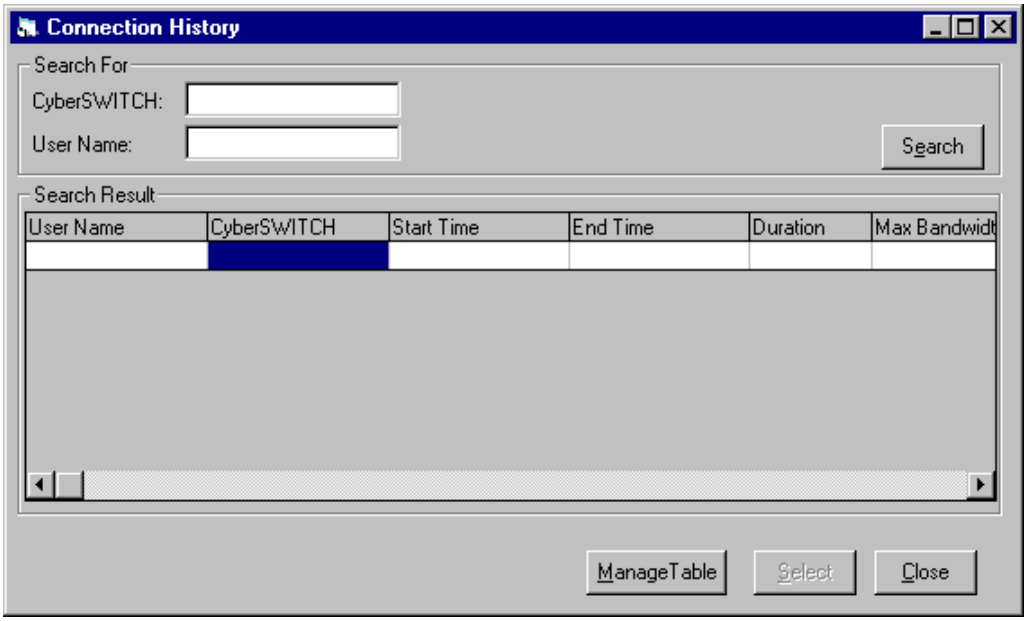
3. To view statistics on a per call basis, double click on the connection.

4. Click *Close* to exit.

CONNECT HISTORY

The Connection History log has similar features to Current Connect. The status of the call is not included, since all past calls are inactive. However, the end time has been added to the table. These statistics can also be viewed on the basis of each call that makes up a connection. The call display also lists the calling number, the called number, and the charges for the call. The connections listed can be specific to a user, to a CyberSWITCH, to any combination of the two, or all users and CyberSWITCH systems.

Note: All references to time are based on the internal clock of the machine on which the database resides.



SEARCH

This button searches the SQL Database for the past connections based on the parameters that you define. You can search for a specific user or a specific Remote Access Switch or both. Leaving a search field blank indicates a search for all in that category.

CALL AND CONNECT HISTORY TABLES

User Name
The remote user which the Remote Access Switch is connected.

CyberSWITCH Name
The Remote Access Switch which the user is connected.

Start Time
The time that this connection was established.

End Time
The time the connection was terminated.

Duration
The total duration, in minutes, of the connection.

Maximum Bandwidth
The maximum bits peer second for the duration of the connection that was established between the user and the Remote Access Switch.

Direction
The direction in which the connection was first established.
- DED stands for a dedicated connection.
- IN stands for a call from the user in to the Remote Access Switch.
- OUT stands for a call from the Remote Access Switch out to the user.

Type
The type of connection currently established. Types include:
- ISDN
- Dedicated
- Digital Modem

Calling Number
The telephone number of the device that initiated the call.

Called Number
The telephone number of the device that was called.

Forwarding
The telephone number that can be used to access the device that was called if the called number is unavailable.

VIEWING PAST CONNECTIONS

1. On the *Functions* menu, select *Connect History*, or click on the toolbar. The *Connect History* dialog appears.

2. Enter a User Name, a CyberSWITCH name, or both and click *Search*.

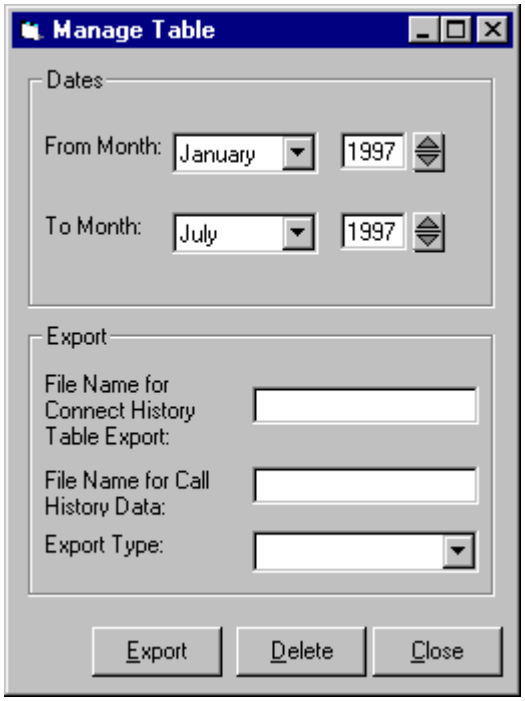
   Note: Leaving a search field blank indicates a search for all in that category.

3. To view statistics on a per call basis, double click on the connection.

4. Click *Close* to exit.

CONNECT HISTORY MANAGER

The Call and Connect History tables continue to grow as more and more users connect with Remote Access Switches managed by SFVRA Connection Manager. In order to keep these tables from growing to an enormous size, the Manage History Table dialog allows you to export call and connection entries to specified files or to simply delete the data. If you are exporting data to a file you must specify a file name for both the Connect History entries and the Call History entries. SFVRA-CONN will create the new files for the data. Data cannot be appended to existing files.



DATES

These fields let you define a time frame for the data that you want to export or clear from the Call and Connect History Tables. The time frames are inclusive, i.e. "From (the beginning of this) Month To (the end of that) Month."

EXPORT FILE NAMES

Specify the names of the files you want created for the data from the Call and Connect History tables.

EXPORT TYPE

Data may be exported to the following formats:

- Record (.ASC)
  A fixed-width text file suitable for importing to client / server and mainframe databases such as DB2.
- Tab-separated (.TSV)
  Tab characters separate fields, and new-line pairs separate records. Character fields are enclosed within double-quote (CHR$(34)) characters.
- Text (.TXT)
  The equivalent of printing the report to the Generic / Text Only (TTY) printer driver to the FILE device.
- DIF (.DIF)
  Data Interchange Format for importation into spreadsheet applications that support the DIF format.
- Comma-separated (.CSV)
  Character fields are enclosed within double-quote characters, and a comma separates each field.

EXPORT
This button exports the data indicated by the dates to the specified files. A file name must be specified for both the Connect History data and the Call History data. The exported data is copied from these tables and placed in a tab delineated file. The data includes what you see in the two tables with the addition of the following:

Connect Number
A unique number assigned by the SFVRA-CONN to the established connection. It is used as the Identity field for the Connect History Table. This number matches calls that correspond to a connection to that connection.

Connect ID
A number assigned by SFVRA-CONN to the established connection.

In Octet Number
The number of octets, eight bit groups, that were transmitted over an inbound call to a Remote Access Switch. The connection octet count is the summation of the inbound octets for all calls that correspond to that connection.

Out Octet Number
The number of octets, eight bit groups, that were transmitted over an outbound call to a Remote Access Switch. The connection octet count is the summation of the outbound octets for all calls that correspond to that connection.

Call Number
A unique number assigned by the SFVRA-CONN to the established call. It is used as the Identity field for the Call History Table.

Call ID
A number assigned by the SFVRA-CONN to the established call.

Advice on Charges
Currently, this feature is only supported on connections to NTT, NET5, and 1TR6 switches. The information delivered by these switches is required to track phone call charges.

CLEAR
This button deletes the data indicated by the dates from the Connect and Call History Tables.

MANAGING THE CALL AND CONNECT HISTORY TABLES

1. On the *Functions* menu, select *Connect History*, or click on the toolbar. The *Connect History* dialog appears.

2. Enter a User Name, a CyberSWITCH name, or both and click *Search*.

   Note: Leaving a search field blank indicates a search for all in that category.

3. Click *Manage Table*

4. Specify a date range, and, if exporting, specify file names.

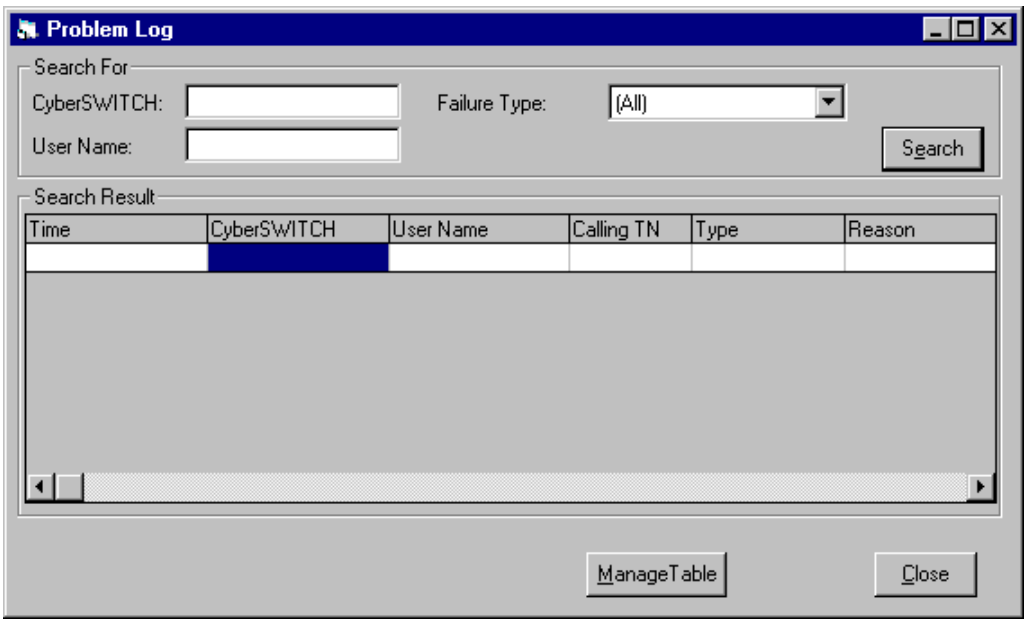
5. Click *Export* or *Delete*.

6. Click *Close* to exit.

PROBLEM LOG

The problem log lists calls chronologically for the time that the problem occurred. It also includes the user name, the CyberSWITCH name, the calling telephone number, the type of failure, and the reason for failing. Failure types include authentication, connection, NAS down, and time restrictions. The problems listed can be specific to a user, to a CyberSWITCH, to a problem type, to any combination of the three, or to all users, CyberSWITCH systems, and problem types.

Note: All references to time are based on the internal clock of the machine on which the database resides.



SEARCH

This button searches the SQL Database for the current connections based on the parameters that you define. You can search for a specific user, a specific Remote Access Switch, a specific failure type, or any combination of the three. Leaving a search field blank indicates a search for all in that category.

PROBLEM LOG TABLE

Problem Time
The date and time the problem occurred.

CyberSWITCH Name
The Remote Access Switch which the user was connected.

User Name
The remote user which the Remote Access Switch was connected.

Start Time
The time that this connection was established.

Failure Type
The type of failure as defined in the SQL Database table FAILURE_TYPES. Failure types include:

- Authenticate failed
- CSX Connection Active
- CSX Keepalive Failure
- Connect failed
- Time restriction

Reason
A string defining the reason for failure as defined in the SQL Database table REASON_STRINGS. Refer to the *System Messages* chapter for more information about the reasons for failure. Reasons include:

- Cannot find this device name
- Error accessing the database
- Password is wrong
- Used wrong authentication
- Exceeded the time limit
- Exceeded the bandwidth limit
- Incorrect Ethernet Address
- No access at this time
- Incorrect connection type
- No channels available
- Invalid calling number
- Invalid secret
- Cannot aggregate this call
- User not part of this group
- No CyberSWITCH configured for this User's group
- CyberSWITCH call back
- CyberSWITCH load level call back
- Too many requests
- CSX Down
- CSX Up

Calling TN
The telephone number of the user that made the connection.

VIEWING THE PROBLEM LOG

1. On the *Functions* menu, select *View Problem Log*, or click on the toolbar. The *Problem Log* dialog appears.

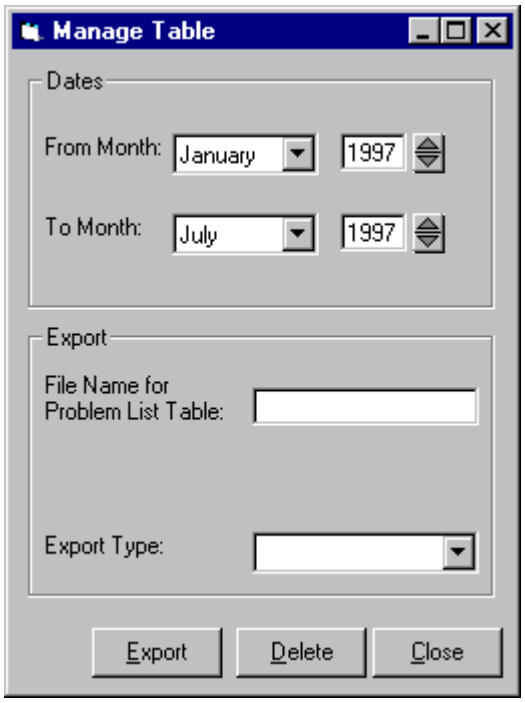
2. Enter a User Name, CyberSWITCH name, failure type, or any combination of the three and click *Search*.

   Note: Leaving a search field blank indicates a search for all in that category.

3. Click *Close* to exit.

PROBLEM LOG MANAGER

The Problem Log continues to grow as more and more users connect with Remote Access Switches managed by SFVRA Connection Manager. In order to keep this table from growing to an enormous size, the Manage History Table dialog allows you to export connection entries to specified files or to simply delete the data. If you are exporting data to a file you must specify a file name. SFVRA-CONN will create the new files for the data. Data cannot be appended to existing files.



DATES

These fields let you define a time frame for the data that you want to export or clear from the Problem Log. The time frames are inclusive, i.e. "From (the beginning of this) Month To (the end of that) Month."

EXPORT FILE NAME

Specify the name of the file you want created for the data from the Problem Log.

EXPORT TYPE

Data may be exported to the following formats:

- Record (.ASC)
  A fixed-width text file suitable for importing to client / server and mainframe databases such as DB2.
- Tab-separated (.TSV)
  Tab characters separate fields, and new-line pairs separate records. Character fields are enclosed within double-quote (CHR$(34)) characters.
- Text (.TXT)
  The equivalent of printing the report to the Generic / Text Only (TTY) printer driver to the FILE device.
- DIF (.DIF)
  Data Interchange Format for importation into spreadsheet applications that support the DIF format.
- Comma-separated (.CSV)
  Character fields are enclosed within double-quote characters, and a comma separates each field.

EXPORT

This button exports the data indicated by the dates to the specified file. The exported data is copied from this table and placed in a tab delineated file. The data includes what you see in the Problem Log with the addition of the following:

Call ID
A number assigned by the SFVRA-CONN to the established call.

Connect ID
A number assigned by SFVRA-CONN to the established connection.

MANAGING THE PROBLEM LOG

1. On the *Functions* menu, select *View Problem Log*, or click on the toolbar. The *Problem Log* dialog appears.

2. Enter a User Name, CyberSWITCH name, failure type, or any combination of the three and click *Search*.

   Note: Leaving a search field blank indicates a search for all in that category.

3. Click *Manage Table*.

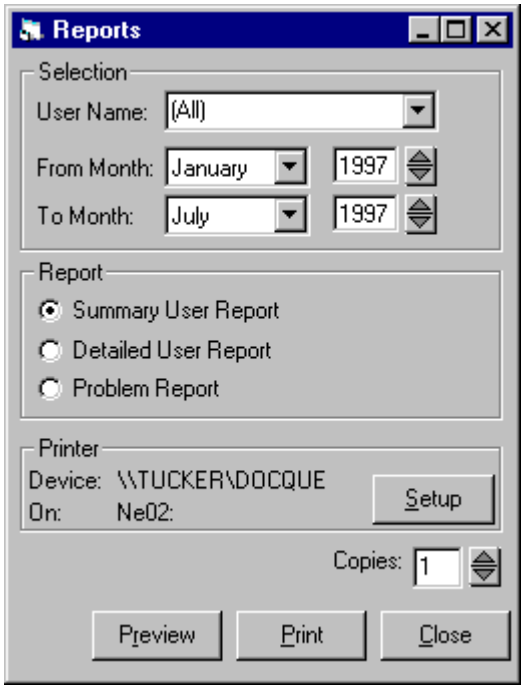
4. Specify a date range, and, if exporting, specify a file name.

5. Click *Export* or *Clear*.

6. Click *Close* to exit.

CONNECTION REPORTS

The SFVRA Connection Manager provides the ability to create and print reports about the connection history and problem log. Connection history reports include a summary report and a detailed report. The problem log report is a summary report. You can select a user, or all users and a time frame for each report. Currently, you must have a default printer configured, even if you are printing to a file, in order to use Reports. Refer to your operating system's documentation on how to install a printer.



The Summary User Report provides minimal information intended for scanning a large number of calls. The information includes the month and year, the user name, the number of connections, the duration of the connections, and the number of calls.

Month
The month and year the connection was established.

User Name
The remote user to which the Remote Access Switch was connected.

Connects
The total number of connections the user made in that month.

Duration
The total time of all the connections the user made that month.

Calls
The total number of calls that made up all the connections the user made that month.

The Detailed User Report provides all information about the connections within the specified time period. The information includes the user name, the CyberSWITCH name, the direction of the call, the type of connection that was made, the number of calls that were made per connection, the maximum bandwidth, the start and end time, the duration of the call, the calling number and the number that was called. This report is sorted by the disconnection time.

User Name
The remote user which the Remote Access Switch was connected.

CyberSWITCH Name
The Remote Access Switch which the user was connected.

Direction
The direction in which the connection was first established.
- DED stands for a dedicated connection.
- IN stands for a call from the user in to the Remote Access Switch.
- OUT stands for a call from the Remote Access Switch out to the user.

Type
The type of connection currently established. Types include:
- ISDN
- Dedicated
- Digital Modem

Calls
The number of calls that make up the connection.

Maximum Bandwidth
The maximum bits peer second for the duration of the connection that was established between the user and the Remote Access Switch.

Start Time
The time and date the connection was established.

End Time
The time and date the connection was terminated.

Duration
The total duration, in minutes, of the connection.

Calling Number
The telephone number of the device that initiated the call.

Called Number
The telephone number of the device that was called.

The Problem Report provides a brief summary of connections that had problems. The information includes the CyberSWITCH name, the date, the user name and the reason for failure.

CyberSWITCH Name
The Remote Access Switch which the user was connected.

Date
The month and year the connection was established.

User Name
The remote user which the Remote Access Switch was connected.

Reason for Failure
A string defining the reason for failure as defined in the SQL Database table REASON_STRINGS. Reasons include:

- Cannot find this device name
- Error accessing the database
- Password is wrong
- Used wrong authentication
- Exceeded the time limit
- Exceeded the bandwidth limit
- Incorrect Ethernet Address
- No access at this time
- Incorrect connection type
- No channels available
- Invalid calling number
- Invalid secret
- Cannot aggregate this call
- User not part of this group
- No CyberSWITCH configured for this User's group
- CyberSWITCH call back
- CyberSWITCH load level call back
- Too many requests
- CSX Down
- CSX Up

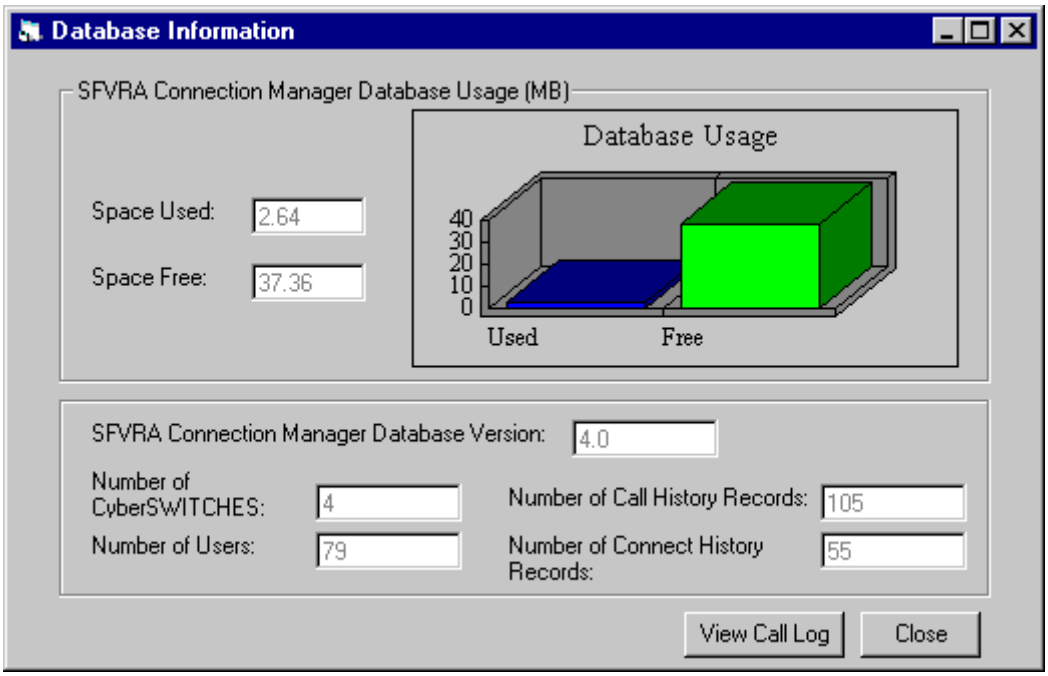
CREATING REPORTS

1. On the *Functions* menu, select *Reports*, or click on the toolbar. The *Reports* dialog appears.
2. Enter the user and time frame for the report.
3. Select type of report.
4. Click *Preview*. A preview of the report is shown.
   - Click to print the report.
   - Click to export the report to a file. Select the file type.
   - Click to export the data to a local email mailbox. Select the file type.

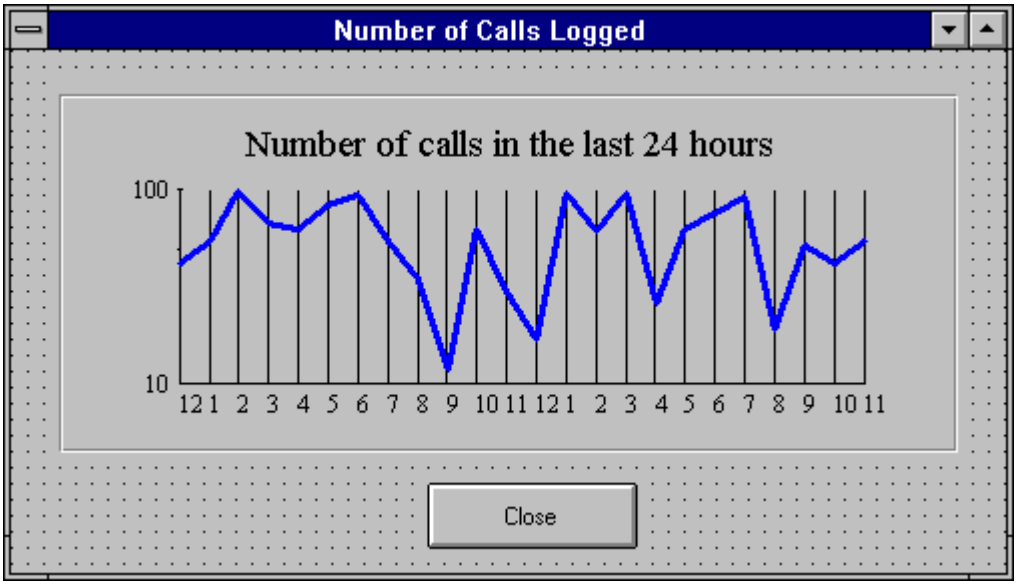
     Note: If you do not have a local email mailbox, you will not be able to proceed after selecting the file type.
5. Click *Close* to exit.

DATABASE INFORMATION

Database Information displays general information about the SFVRA Connection Manager and its database. This is useful for determining whether the available space on the database needs to be cleared. If the database runs out of space, SFVRA-CONN will continue to function, but will not be able to log calls or problems. Call restriction polices may suffer as well. Database Usage displays a graphical representation of how much hard drive space, in MB, is being used and how much is free. Additional information includes the version number of the SFVRA-CONN, the number of Users and CyberSWITCH systems that are configured in the database, the number of calls that are currently on record, and the number of past connections that are currently on record.



The Call Log displays a line graph of the number of calls made in the last 24 hours with respect to the time the call was placed.



Note: All call times are rounded down. For example, any calls made between 4:00 and 4:59 are counted and marked at 4:00.

VIEWING DATABASE INFORMATION

1. On the *Functions* menu, select *Database Information*, or click on the toolbar. The Database Information dialog appears.

2. Click *View Call Log* to see calls from the last 24 hours.

3. Click *Close* to exit.

ROUTINE MAINTENANCE

OVERVIEW

This chapter provides instructions for performing routine SFVRA Connection Manager maintenance such as:

- performing a configuration back up
- upgrading the application software
- upgrading the database software

CONFIGURATION BACK UP

The SFVRA-CONN's database data and the SFVRA-CONN application's data is critical to the SFVRA Connection Manager's operation. We strongly suggest that you back up this data in case you ever need to restore it.

The SFVRA-CONN's database data is stored by the MS SQL Server. Use the available MS SQL Server tools to perform backups of the SFVRA database.

As a default, the SFVRA-CONN's application configuration data is stored on the same hard drive where the application is installed. The default path is as follows:

```
C:\Program Files\Sfvra\Program
```

Use available Windows 95/NT tools to back up this directory. Fro example use the Windows 95/NT Explorer to make a copy of the `Program` directory, then store the copy of the directory for backup purposes.

UPGRADING THE SFVRA-CONN SOFTWARE

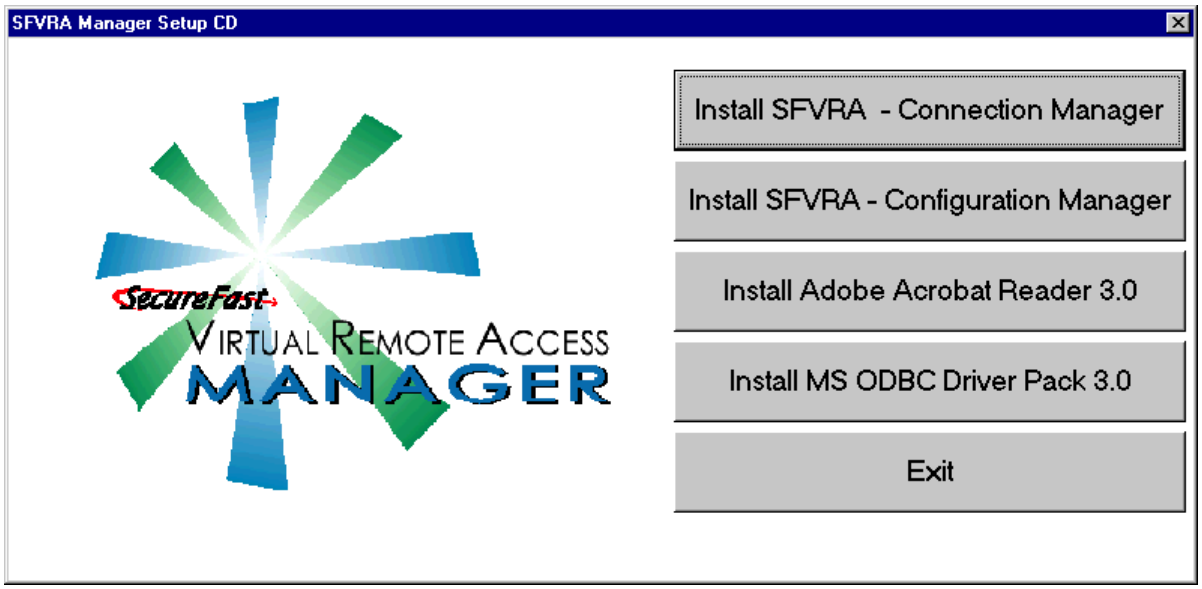
The utility used to upgrade the SFVRA-CONN software checks which components of the Client and Service are installed. You are given the option to update only the components that have been previously installed, or to upgrade the installed components and select additional components to be installed. The service is stopped and deleted before it is updated. If you have indicated that the SQL Server Database is located on this machine, the update procedure also checks if the database needs to be updated. A message will indicate if the database needs to be updated. Upgrades should be performed at all instances of the SFVRA Connection Manager, whether the machines support the Client, the Services, the Database, or any combination of the three. During the software upgrade, you will be given the option of upgrading:

- Client Files includes the software for the Client Interface, the Manage Logins application, the CSX Monitor application, and the Convert application.
- SQL Setup application aids in the creation of SFVRA database files for the Microsoft SQL Server. The SQL Setup application should only be installed on the PC running the MS SQL Server.
- Service Files includes the SFVRA Service, the SFVRA RIP Service, and the SFVRA Proxy ARP Service.
- The SFVRA Connection Manager Documentation installs the User's Guide.

Upgrade the SFVRA-CONN software using the following steps:

1. Close any active applications.

2. Insert the SFVRA Manager Setup CD into the CD-ROM drive. If, as is usually the case, you CD-ROM is setup for AutoRun, the following screen will be displayed.



To manually load the above screen, select *Run* from the Start Menu. Enter *<CD-ROM drive>:\SCCD.EXE* as the program to open, then select *OK*.

3. Click *Install SFVRA Connection Manager.*

4. At the prompt, determine whether the SFVRA SQL Server Database is installed on this machine.

5. Follow the onscreen instructions to complete the upgrade.

UPGRADING THE SFVRA DATABASE

The following instructions briefly discuss upgrading the SFVRA Database. Refer to the *SQL Setup Utility* chapter for more information.

1. Login to the MS SQL Server. Enter the Login ID *sa* and a password, if necessary, and click *OK*. The SQL Setup program executes.

2. The SQL Server Setup Utility first locates the SFVRA database.

3. Click *OK* to upgrade the database.

4. When the upgrade procedure is complete, MS SQL Server messages are displayed. Ensure that no errors occurred. Scroll through the list of SQL Server Messages, if any.

5. Click *Close*.

SYSTEM VERIFICATION

OVERVIEW

After the SFVRA Connection Manager has been configured, and before proceeding with normal system operation, it is necessary to verify that the system is functional. This chapter provides instructions for verifying the system configuration.

You only need to perform the verification procedures for the options that apply to your configuration. For example, if your configuration does not use CyberSWITCH - User Groups, skip the CyberSWITCH - User Groups verification section.

Note: At least one CyberSWITCH and one remote device is required to proceed with the verification process.

VERIFYING A TCP CONNECTION TO SFVRA

The follow sections provide methods of verifying a TCP connection can be established or is already established between the CyberSWITCHES and the SFVRA-CONN.

VERIFYING THE POSSIBILITY OF A TCP CONNECTION

To verify that a TCP connection can be established between a CyberSWITCH and SFVRA-CONN:

Determine if the CyberSWITCH can access SFVRA-CONN. If the IP Address of the SFVRA Service is 100.0.0.2, at a CyberSWITCH console, type:

ip ping 100.0.0.2 <return>

This command will display a message similar to the following:

```
100.000.000.002 is alive
```

If the system displays this message, then a TCP connection can be established. Repeat this step for each SFVRA Service.

If this message IS NOT is displayed, then a TCP connection can not be established. Refer to the *TCP Connections* section of the *Problem Diagnosis* chapter.

VERIFYING AN EXISTING TCP CONNECTION

To verify that a TCP connection has been established:

Determine the SFVRA Service that should have an established TCP connection with a CyberSWITCH. Assume that the IP Address of the SFVRA Service is 100.0.0.2 and the TCP Port of the CyberSWITCH is 2000. Type,

tcp conns <return>

This command will display a message similar to the following:

```
lport   fhost             fport   window (l/r)   tstate         outq (s/u)
-----   ---------------   -----   ------------   ------------   -------------
2000    100.0.0.2         1253    1182\8696      Established    0/0
```

If the system displays this message, then a TCP connection has been established. Repeat this step for each SFVRA Service.

Note: The lport values should correspond with the TCP Port number configured for this CyberSWITCH, the fhost value should be the IP address of the SFVRA Service, and the tstate value should be Established. All other values may vary from machine to machine.

If the `tstate` IS NOT `Established`, then a TCP connection can not be established. Refer to the *TCP Connections* section of the *Problem Diagnosis* chapter.

VERIFYING THAT SFVRA-CONN HAS BEEN ENABLED ON A CYBERSWITCH

To verify that SFVRA Connection Manager has been successfully enabled on a CyberSWITCH:

Determine the CyberSWITCH that should have SFVRA-CONN enabled. Assume that the IP Address of the SFVRA Service is 100.0.0.2 and the TCP Port of the CyberSWITCH is 2000. Type,

`tcp conns` <return>

This command will display a message similar to the following:

```
lport   fhost             fport   window (l/r)   tstate         outq (s/u)
-----   ---------------   -----   ------------   ------------   -------------
2000    100.0.0.2         1253    1182\8696      Listen         0/0
```

If the system displays this message, then SFVRA-CONN has been successfully enabled on the CyberSWITCH. Repeat this step for each CyberSWITCH.

If the `tstate` IS NOT `Listen` or `Established`, then a SFVRA-CONN has not been properly enabled for this CyberSWITCH. Refer to the Remote Access Switch's documentation to properly enable SFVRA Connection Manager.

VERIFYING GROUP ASSIGNMENTS

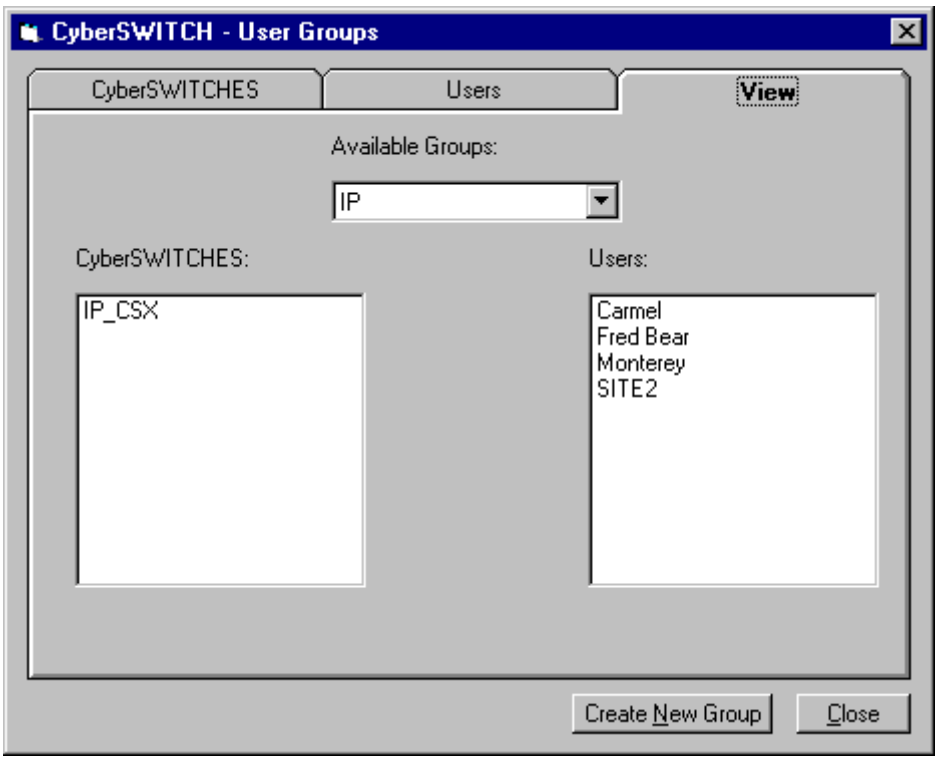
To verify that CyberSWITCH systems and Users have been properly assigned to a group:

1. On the *Functions* menu, select *CyberSWITCH - User Grouping*, or click on the toolbar.

2. Select the *View* tab.

3. Select an available group.

   The CyberSWITCH systems and Users configured in the group are listed. For example, if you are verifying a group called "IP" that contained the CyberSWITCH IP_CSX and the users Carmel, Fred Bear, Monterey and SITE2, the View tab would appear as follows:



4. Ensure that there are no CyberSWITCH systems or Users that are missing or that don't belong.

5. Click *Close*.

PROBLEM DIAGNOSIS

OVERVIEW

This chapter, when used in conjunction with the *System Verification* chapter, helps diagnose problems encountered in the verification process.

TCP CONNECTIONS

Problem:
The CyberSWITCH connected to the same LAN as SFVRA Connection Manager does not receive a ping response from the SFVRA Service.

Action:

1. Verify that the SQL Service is running. Under the Control Panel of the machine with the SQL Server, select *Services*. Ensure that the SQL Server is listed as *Started*. If the SQL Server is not running, refer to the appropriate Microsoft documentation in order to start the server.

2. Verify that the SFVRA Service is running and that it can access the SQL database. Under the Control Panel of the machine with the SFVRA Service, select *Services*. Ensure that the SFVRA Service is listed as *Started*. If the SFVRA Service is not running, refer to *Starting and Stopping the SFVRA-CONN Services*. Under the Control Panel, select *32-bit ODBC*. Ensure that the ODBC driver parameters are correct.

3. Verify that no errors occurred with the SFVRA Service or SQL Server. From the Start Menu, select Programs / Administrative Tools (Common) and then select *Event Viewer*. Ensure that there are no SQL-related or SFVRA-related errors listed.

   Note: You may want to clear the log first, then reboot the machine or stop and then start the SFVRA Service to get fresh data.

4. Ensure that the IP address for the CyberSWITCH system's LAN interface and the TCP Port number are accurate in the SFVRA Database. From the SFVRA Client's File menu, select *CyberSWITCH*.

5. Verify on the CyberSWITCH that device level authentication is enabled, *VRA Manager* has been selected for the off-node device database location, and that the TCP Port number is correct.

6. Verify that the LAN is functional.

Problem:
There are two SFVRA Services listed at the same IP address after issuing a *tcp conns* command.

Action:

1. Reissue the command: `tcp conns`. More than likely one of the two connections was lost and the second was reestablished. The first connection had not yet been deleted from memory.

SYSTEM MESSAGES

OVERVIEW

This chapter describes the types of system messages available. There are three categories of these messages based on where they are generated: the Client interface, the SQL database, and the Problem Log.

The Client interface messages are divided into four types: error, warning, informational and interrogative. These messages have the title *SFVRA Connection Manager:<Number>*. The type of message is indicated by the number and by different symbols on the dialog box. Messages are numbered using the following scheme:

Error Messages:	1000-1999
Warning Messages:	2000-2999
Informational Messages:	3000-3999
Interrogative Messages:	4000-4999

Each message is listed individually, grouped by type, and listed by number with suggested actions to take in the event of an error.

Other messages that you may encounter are SQL errors and are numbered by the SQL manufacturer. These numbers have the prefix RDO (Remote Data Object). Refer to Microsoft SQL Administrator Companion for more detail.

The Problem Log lists messages that pertain to problems with connections to the SFVRA database. This chapter lists each problem type, a description of the corresponding failure message with possible solutions.

CLIENT INTERFACE MESSAGES

ERROR MESSAGES

Error messages signal that a procedure failed. These messages are indicated by on the dialog box and contain a description of each error message and suggestions for a resolution.

SFVRA Connection Manager: 1000 A Login ID must be entered.
The login operation failed because no Login ID was provided. Check with your system administrator to get the proper Login ID.

SFVRA Connection Manager: 1001 This version of the SFVRA Connection Manager Client requires SFVRA database version: <version> or later. The current SFVRA database version is: <current_version>.
The SFVRA-CONN Client requires the SFVRA database version to be the same or later. This error occurs when the Client interface has been upgraded and the database has not. If the Client interface has a later version than the database, the Client will connect to the database, but you will be unable

to view or change any information. We recommend that you upgrade the SFVRA database before upgrading the SFVRA-CONN Clients to avoid this error.

Note: Version 2 Client software can only connect to version 2 of the SFVRA database.

SFVRA Connection Manager: 1002 System Information is unavailable at this time.
The User Data Source is not defined as a valid user of a trusted SQL server connection, or the connection to the SQL Server has been dropped since the last action. Ensure under the Control Panel, 32-bit ODBC, that the User Data Source for "SFVRA" does not have the "Use Trusted Connection" box checked, or that the server allows this user with a Trusted Connection.

SFVRA Connection Manager: 1003 The Base Data Rate cannot be 56000 while H0 Call Support is enabled.
H0 Call support demands a Base Data Rate of 64000 bps. If you need a Base Data Rate of 56000 bps, disable H0 Call Support first.

SFVRA Connection Manager: 1004 IP Address cannot be NULL.
The IP Address of the CyberSWITCH'S LAN port must be included before the CyberSWITCH can be added to the database as a Remote Access Switch. The SFVRA service will be unable to locate the CyberSWITCH without an IP Address.

SFVRA Connection Manager: 1005 TCP Port cannot be NULL.
The TCP Port number is used by the SFVRA service to establish a connection with the CyberSWITCH and must be included before the CyberSWITCH can be added to the database as a Remote Access Switch.

SFVRA Connection Manager: 1006 Reserved ISDN channels exceeds number of ISDN channels.
The number of channels reserved for Priority Users cannot exceed the number of channels available within a connection type.

SFVRA Connection Manager: 1007 Reserved Modem channels exceeds number of Modem channels.
The number of channels reserved for Priority Users cannot exceed the number of channels available within a connection type.

SFVRA Connection Manager: 1008 Start IP Address cannot be NULL.
A Start IP Address must be defined before IP Pool Addressing is enabled.

SFVRA Connection Manager: 1009 End IP Address cannot be NULL.
An End IP Address must be defined before IP Pool Addressing is enabled.

SFVRA Connection Manager: 1010 Start IP Address must be less than the End IP Address.
The IP Pool Addressing function failed. Reconfigure the address pool range so that the Start IP Address is less than the End IP Address.

SFVRA Connection Manager: 1011 From month cannot be greater than To month.
Invalid time frame. Reconfigure the time frame so that the "From" occurs before the "To" in the calendar year.

SFVRA Connection Manager: 1012 From year cannot be greater than To year.
Invalid time frame. Reconfigure the time frame so that the "From" year is less than or equal to the "To" year.

SFVRA Connection Manager: 1013 METRIC must be a value between 1 and 16.
Invalid metric number. Reconfigure the metric to fall in the indicated range.

SFVRA Connection Manager: 1014 The Login ID specified does not have access to the SFVRA database.
Login failed. The Login ID is valid, however, it does not have permission to access the database. From the Control Panel, open ODBC. Ensure that Use Trusted Connection is turned off. If the Login ID was crested within the SQL server, ensure that the user has permission to access the database.

SFVRA Connection Manager: 1016 File already exists. Please choose new filename.
Export failed. The export function cannot append data to a previously created file. Choose a different file name or directory.

SFVRA Connection Manager: 1017 Cannot get current time from database.
Indicates that the duration of a current connection cannot be determined because the SQL service is down or cannot be reached by this machine. Ensure that the SQL server is running properly and that the network integrity has been maintained.

SFVRA Connection Manager: 1018 No CyberSWITCH selected to DELETE.
Deletion failed. A CyberSWITCH must be selected in order to perform this function.

SFVRA Connection Manager: 1019 No CyberSWITCH selected to DUPLICATE.
Duplication failed. A CyberSWITCH must be selected in order to perform this function.

SFVRA Connection Manager: 1020 Unable to DELETE, as there are currently calls to this CyberSWITCH.
Deletion failed. A CyberSWITCH cannot be removed from the database while there is a current connection with the CyberSWITCH.

SFVRA Connection Manager: 1021 Unable to DELETE, as there are currently calls to this User.
Deletion failed. A user cannot be removed from the database while there is a current connection with the user.

SFVRA Connection Manager: 1022 This User Name already exists in the database.
A User Name must be unique. Currently the database is not case sensitive. Choose a different User Name.

SFVRA Connection Manager: 1023 Invalid time format. Enter time in the format "hh:mm".
Call Restrictions configuration error. The time format is based on a 24 hour clock, where hh stands for 00 to 23 and mm stands for 00 to 60.

SFVRA Connection Manager: 1024 Minutes/Call < Minutes/Day < Minutes/Month.
Call Restrictions configuration error. The maximum minutes per call restriction must be less than the maximum minutes per day restriction. The maximum minutes per day restriction must be less than the maximum minutes per month restriction.

SFVRA Connection Manager: 1025 End Time must be greater than Start Time.
Call Restrictions configuration error. Invalid time frame. Reconfigure the Start time to be less than the End Time.

SFVRA Connection Manager: 1026 Maximum Bandwidth must be greater than or equal to Initial Bandwidth.
Invalid bandwidth configuration. The Initial Bandwidth must be less than the Maximum Bandwidth.

SFVRA Connection Manager: 1027 Invalid IPX Network Number. Enter a hexadecimal number between 0 and FFFFFFFE (0 for none).
Reconfigure the Network Number to be within the defined parameters.

SFVRA Connection Manager: 1028 Invalid AppleTalk Address
An AppleTalk Address consists of the network number followed by a node ID.

SFVRA Connection Manager: 1029 File names must be unique.
Export Failed. The data files destined to contain the Connect History and Call History data must be unique. You can not export this data to the same file.

SFVRA Connection Manager: 1030 Invalid file name.
Export Failed. The destination data file names must follow the DOS rules for file naming.

SFVRA Connection Manager: 1031 Callable and Callback can only be ENABLED if there is a telephone number configured.
In order for these features to work, a telephone number must be assigned to the user. These features cannot be enabled without a telephone number.

SFVRA Connection Manager: 1032 This ADD only available in User UPDATE mode. Please ADD the user first.
Certain features, such as Telephone Numbers, are written directly to the database upon configuration. The user must be previously defined in the database before these features can be written. Add the user to the database and return to the field in question in the UPDATE mode.

SFVRA Connection Manager: 1033 A Computer Name must be entered.
The SFVRA Service requires the Computer Name of the machine that runs the Network Proxy Service in order to send information about current connections for the services to advertise.

SFVRA Connection Manager: 1034 Invalid Export type.
The specified file is not a valid file type for export with this program. Valid files types are: records (.ASC), tab-separated (.TSV), text (.TXT), Data Interchange Format (.DIF), and comma-separated (.CSV).

SFVRA Connection Manager: 1035 The item being accessed no longer exists in the database.
The item, either a CyberSWITCH or a User, was deleted from the database by another administrator. The CyberSWITCH and User Lists are not dynamic, therefore this can happen using the Select, Update, and Delete buttons.

SFVRA Connection Manager: 1036 Invalid IP Address. Use the format ###.###.###.###.
Each IP Address must be configured in the dotted decimal format, where ### represents numbers 0-254.

SFVRA Connection Manager: 1037 The IP Address is already associated with an SFVRA Service.
Only one SFVRA Service may be associated with an IP Address. Ensure that the IP address for the SFVRA Service is correct.

SFVRA Connection Manager: 1038 This ADD only available in CyberSWITCH UPDATE mode. Please ADD the CyberSWITCH first.
In order to add a user to a CyberSWITCH'S Priority User list, the CyberSWITCH must be previously configured in the database. Click *Add* at the bottom of the dialog to write the CyberSWITCH information to the database, and then click *Add* in the ISDN Users box or in the Modem Users box to configure Priority Users.

SFVRA Connection Manager: 1039 CyberSWITCH Name cannot be left blank.
A CyberSWITCH Name must be specified before adding a CyberSWITCH to the database. This CyberSWITCH Name does not necessarily need to be the same as the System Name configured on the CyberSWITCH.

SFVRA Connection Manager: 1040 User Name cannot be left blank.
A User Name must be specified before adding a User to the database. This User Name must match the System Name of the remote device that contacts the central site CyberSWITCH systems.

SFVRA Connection Manager: 1041 Reports not available. You must set a default printer.
A default printer must be assigned in order for Reports to function, even if you plan to print to a file. Configure a printer for the PC or network.

SFVRA Connection Manager: 1042 This CyberSWITCH Name already exists in the database.
A CyberSWITCH Name must be unique. Currently the database is not case sensitive. Choose a different CyberSWITCH Name.

SFVRA Connection Manager: 1043 Number must be numeric.
Addition of a Telephone Number or Calling Line ID failed. The number must not contain non-numeric characters.

SFVRA Connection Manager: 1044 Invalid TCP Port value.
Reconfigure the TCP Port value to be numeric.

SFVRA Connection Manager: 1045 Name cannot be blank and cannot exceed 16 characters.
In order to configure a User Category or a CyberSWITCH - User Group, the name must be at least one character in length, and not exceed 16 characters. Rename the category or group.

SFVRA Connection Manager: 1046 This entry already exists in the table.
A User Category name and a CyberSWITCH - User Group name must be unique. Currently the database is not case sensitive. Configure a new name for the User Category or CyberSWITCH - User Group.

SFVRA Connection Manager: 1047 Unable to add entry containing the single quote (') character.
The User Category name and the CyberSWITCH - User Group name can contain any printable character except the single quote (') character. Re-enter the name so that it does not use the single quote (') character.

SFVRA Connection Manager: 1048 This Group has already been configured for another Network Proxy Service. A Group can only be configured for one Network Proxy Service.
Groups can only be configured for one Network Proxy service so that routes are not advertised by multiple servers and, therefore, accessed by differing CyberSWITCH systems.

WARNING MESSAGES

Warning messages signal events that you should investigate. These messages are indicated by on the dialog box, and may be normal during certain network conditions, or they may indicate a problem. The SFVRA-CONN should continue to operate after posting a warning message. There are currently no warning messages.

INFORMATIONAL MESSAGES

SFVRA-CONN provides several informational messages. The messages are indicated by on the dialog box and contain information mainly pertaining to actions that are a result of an action that the administrator provoked.

SFVRA Connection Manager: 3000 The Base Data Rate, Initial Bandwidth, and Maximum Bandwidth may have been changed by enabling this option.
H0 Call Support demands that the Base Data Rate is set to 64000 bps. If the Base Data Rate has been configured for 56000 bps, enabling H0 Call Support will automatically change it to 64000 bps, and the Initial Bandwidth and Maximum Bandwidth will be changed 384000 bps.

SFVRA Connection Manager: 3001 Protocol Callable field(s) have been disabled.
A user cannot have Callable enabled if there are no Telephone Numbers configured. Deleting the last Telephone Number results in disabling any Callable fields.

SFVRA Connection Manager: 3002 The Callback feature for this user has been disabled.
A user cannot have Callback enabled if there are no Telephone Numbers configured. Deleting the last Telephone Number results in disabling the Callback feature.

SFVRA Connection Manager: 3003 No lines to report with current selection.
There is no information saved in the database about the time frame indicated. No report will be created.

SFVRA Connection Manager: 3004 No calls registered for the selected connection.
The Current Connections table is not updated dynamically. Once a connection has been terminated, the record of the call is placed in the Connect History table. However, if the Current Connections dialog is active the connection will still appear in the table. Furthermore, if the connection is selected to view the corresponding calls, the database will be unable to locate the information, since it has been moved to the Connect History table.

SFVRA Connection Manager: 3005 No lines to EXPORT with current selection.
There is no information saved in the database about the time frame indicated. No data will be exported to the indicated file(s).

SFVRA Connection Manager: 3006 This User has been removed from the Priority Users List due to a change in its Connect Type.
The User was previously configured as a Priority User. Changing the type of connection used removes the user from the Priority User List for that connection type. The user must be reconfigured into the Priority User List under the new connection type, if desired.

SFVRA Connection Manager: 3007All Priority Users must be deleted prior to changing the CyberSWITCH'S group.
This CyberSWITCH currently has Priority Users. These users will be unable to access this CyberSWITCH if the group is reconfigured. Delete the Priority Users before reconfiguring the CyberSWITCH'S group.

SFVRA Connection Manager: 3008 Nothing has been SELECTED.
In order to perform the selected function, such as deleting a telephone number, data must be selected.

SFVRA Connection Manager: 3009 No User selected to DUPLICATE.
In order to duplicate a user, one must be configured in the database.

SFVRA Connection Manager: 3010 The <No Group> group cannot be DELETED.
The <No Group> group is the default group of all CyberSWITCH systems and Users that have not been assigned to a specific group, and, therefore, cannot be deleted.

INTERROGATIVE MESSAGES

Interrogative messages provide a last call before performing an action. These messages are indicated by on the dialog box.

Are you sure you want to UPDATE?
Indicates that changes have been made that will be saved to the database.

SFVRA Connection Manager: 4000 CLEAR without saving your changes?
Indicates that changes have been made that will not be saved to the database.

SFVRA Connection Manager: 4001 CLOSE without saving your changes?
Indicates that changes have been made that will not be saved to the database.

SFVRA Connection Manager: 4002 RESET the Day and Month totals to zero?
Indicates that the users call restriction will be reset to zero for this month. You will be unable to undo the reset.

SFVRA Connection Manager: 4003 Are you sure you want to ADD the user to the group(s)?
Indicates that the user will be included into the selected group(s). Ensure that each CyberSWITCH within the group is available to handle the protocol(s) of the user.

SFVRA Connection Manager: 4004 Are you sure you want to DELETE the user from the group(s)?
Indicates that the user will be removed from the selected group(s). Ensure that the user has access to at least one CyberSWITCH after removing it from a group.

SFVRA Connection Manager: 4005 DELETE entries from Connect_History and Call_History database tables?
Indicates that information will be removed from the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4006 DELETE entries form Problem List database tables?
Indicates that information will be removed from the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4007 Are you sure you want to ADD to the group?
Indicates that the selected CyberSWITCH(ES) or User(s) will be included into the selected group. Ensure that each CyberSWITCH within the group is available to handle the protocol(s) of the user.

SFVRA Connection Manager: 4008 Are you sure you want to DELETE from the group?
Indicates that the selected CyberSWITCH(ES) or User(s) will be removed from the selected group(s). Ensure that the user has access to at least one CyberSWITCH after removing it from a group.

SFVRA Connection Manager: 4009 ADD CyberSWITCH: <CyberSWITCH Name> to the database?
Indicates that a new CyberSWITCH will be added to the database as a new Remote Access Switch. Ensure that the CyberSWITCH is properly configured.

SFVRA Connection Manager: 4010 UPDATE: <CyberSWITCH Name>?
Indicates that changes have been made to the named CyberSWITCH that will be saved to the database.

SFVRA Connection Manager: 4011 DELETE CyberSWITCH: <CyberSWITCH Name> from the database?
Indicates that the named CyberSWITCH will be deleted from the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4012 ADD User: <User Name> to the database?
Indicates that a new User will be added to the database. Ensure that the User is properly configured.

SFVRA Connection Manager: 4013 UPDATE: <User Name>?
Indicates that changes have been made to the named User that will be saved to the database.

SFVRA Connection Manager: 4014 DELETE User: <User Name> from the database?
Indicates that the named User will be deleted from the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4015 DELETE table entry: <Entry Name> from the database?
Indicates that the named table entry will be deleted form the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4016 ADD Number: <Number> for User Name <User Name> to the database?
Indicates that the Number will be added to the database as a Telephone Number or CLID. Ensure that the number is functional.

SFVRA Connection Manager: 4018 DELETE Number: <Number> from the database?
Indicates that the Number will be deleted from the database. This information cannot be recovered once it is deleted, and may affect other configurations, such as the Callable and Callback features.

SFVRA Connection Manager: 4019 ADD IP Static Route: <Destination IP Address> for User Name <User Name> to the database?
Indicates that the named IP Static Route will be added to the database. Ensure that the route information is accurate.

SFVRA Connection Manager: 4020 DELETE IP Static Route: <Destination IP Address> from the database?
Indicates that the named static route will be deleted from the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4021 ADD Priority User: <User Name> to the database?
Indicates that the named User will be added to the database as a Priority User for the selected CyberSWITCH.

SFVRA Connection Manager: 4022 DELETE Priority User: <User Name> from the database?
Indicates that the named User will be deleted from the database as a Priority User for the selected CyberSWITCH.

SFVRA Connection Manager: 4023 Priority Users have been configured for this CyberSWITCH that are not in the same group. Do you want them to be DELETED? (You cannot CLEAR or CLOSE until the groups match.)

SFVRA Connection Manager: 4024 ADD Network Proxy Service: <Network Proxy Service> to the database?
Indicates that the named Network Proxy Service will be added to the database. Ensure that the IP Address for the service is valid and a group has been properly assigned.

SFVRA Connection Manager: 4025 UPDATE Network Proxy Service: <Network Proxy Service>?
Indicates that changes have been made to the named Network Proxy Service that will be saved to the database.

SFVRA Connection Manager: 4025 DELETE Network Proxy Service: <Network Proxy Service> from the database?
Indicates that the named Network Proxy Service will be deleted from the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4026 There are Network Proxy Services configured for this Group. Do you want them to be DELETED?
Indicates that the group that has been selected for deletion is currently assigned to a Network Proxy Service. Selecting *Yes* will not only delete the specified group, but will also remove the Network Proxy Service from the database.

SFVRA Connection Manager: 4027 ADD SFVRA Service: <SFVRA Service IP Address> to the database?
Indicates that the named SFVRA Service will be added to the database. Ensure that the IP address for the service is valid.

SFVRA Connection Manager: 4028 UPDATE SFVRA Service: <SFVRA Service IP Address>?
Indicates that changes have been made to the named SFVRA Service that will be saved to the database.

SFVRA Connection Manager: 4029 DELETE SFVRA Service: <SFVRA Service IP Address> from the database?
Indicates that the named SFVRA Service will be deleted from the database. This information cannot be recovered once it is deleted.

SFVRA Connection Manager: 4030 There are Network Proxy Services configured for this group. Do you want them to be deleted?
Indicates that the group that will be deleted from the database has at least one Network Proxy Service assigned to it. If you would like to keep the Network Proxy Service, reconfigure it to be assigned to another group before deleting the group.

SQL ERROR MESSAGES

Data Source Name 'SFVRA' not found.
Under the Control Panel, select 32-bit ODBC. Ensure that there is a User Data Source with the Data Source Name of 'SFVRA.'

The Server defined for the Data Source Name 'SFVRA' cannot be found.
Under the Control Panel, select 32-bit ODBC. Ensure that the User Data Source for "SFVRA" has a valid server listed and the server is accessible.

The Login ID or Password is incorrect.
Check with your system administrator to ensure their validity.

A table in the SFVRA database cannot be accessed.
Under the Control Panel, select 32-bit ODBC. Ensure that the User Data Source for "SFVRA" has the database name set to "SFVRA". Verify all tables have been created in the SFVRA database. Verify the Login ID is in either the "SFVRARW" or "SFVRARO" SQL groups.

ODBC Data Source Name unable to use trusted connection.
Under the Control panel, select 32-bit ODBC. Select the Data Source Name (DSN) specific to your SFVRA-CONN. Ensure that Use Trusted Connection has been disabled by removing the check in the checkbox.

PROBLEM LOG MESSAGES

FAILURE MESSAGES

System failure messages indicate that there has been a problem with a connection to a user or with a CyberSWITCH. The following is a list of Failure types listed in the database PROBLEM_LIST table:

- Authenticate failed
- Connect failed
- Time restriction
- CyberSWITCH Down
- CSX Down
- CSX Up

REASONS FOR FAILURE

The reasons for failure work in conjunction with the Failure types. While the Failure Type is listed in the PROBLEM_LIST table, a corresponding reason is listed in the REASON_STRING table. The following is a list of Reasons for Failure:

Cannot aggregate this call.
Connect Failed. In a Hunt Group situation, SFVRA-CONN aggregates calls across multiple CyberSWITCHES. Ensure Hunt Group phone number is specific to one CyberSWITCH.

Cannot find this device name.
Authenticate Failed. The call from the user was rejected because the user name is not defined in the SQL database. Configure this device name in the SQL database and try to connect again.

CSX Connection Active
CSX Up. The SFVRA Service has a connections to the CyberSWITCH.

CSX Keepalive failure
CSX Down. The SFVRA Service lost the connection to the CyberSWITCH.

CyberSWITCH call back.
The user was successfully authenticated. However, since the Callback feature was enabled for the user, the connection was dropped and re-established by a CyberSWITCH.

CyberSWITCH load level call back.
The user was successfully authenticated. However, since the Load Level feature was enabled for the user, the connection was dropped and re-established by a CyberSWITCH with less current connections.

Error accessing the database.
Authenticate Failed or Connect Failed. The CyberSWITCH was unable to receive authorization to accept the call because it was unable to communicate with SFVRA-CONN. Ensure the physical connection between the CyberSWITCH and the SFVRA-CONN is intact.

Exceeded the bandwidth limit.
Connect Failed. The call from the user was rejected or disconnected because the bandwidth limitation was exceeded for the user. Reconfigure the user to allow a higher bandwidth, or demand that the user request a bandwidth within the limitation.

Exceeded the time limit.
Connect Failed. The call from the user was rejected or disconnected because the of a time limit restriction. You may reconfigure the user with additional time without changing the cumulative statistics or you may reset the cumulative statistics for the user.

Incorrect Ethernet Address.
Authenticate Failed. The call from the user was rejected because the Ethernet Address was incorrect. Ensure that the Ethernet Address configured on the user matches the address in the database.

Invalid calling number.
Connect Failed. The call from the user was rejected based on an invalid Calling Line ID. Ensure that the CLID configured on the user matches the CLID in the database.

Invalid secret.
Authenticate Failed. The call from the user was rejected based on an invalid secret. Ensure that the CHAP secret configured on the user matches the CHAP Secret in the database.

No access at this time.
Connect Failed. The call from the user was rejected or disconnected because of the time of day. Reconfigure the user's Time of Day restriction to allow the call.

No channels available.
Connect Failed. No channels on a CyberSWITCH within the user's group are available to preform the call out function.

No CyberSWITCH configured for this User's group.
A call from a local machine attempted to reach a user in a group that has no CyberSWITCHES. Reconfigure the user to be a part of a different group, or add a CyberSWITCH to the user's group.

Password is wrong.
Authenticate Failed. The call from the user was rejected based on an incorrect password. Ensure that the password configured for the user matches the password configured in the database.

Too many connect requests.
Connect Failed. The call from the user was rejected because the database was overloaded by too many connection requests at one time. Attempt the connection again.

Used wrong authentication.
Authenticate Failed. The call from this user was rejected based on an incorrect authentication method. Ensure that the authentication type for the user matches the authentication type configured in the database.

User not part of this group.
Connect Failed. The call from the user was rejected because it is not part of the same group as the CyberSWITCH that the user attempted to call. Reconfigure the user to be included in the desired group, or have the user call a CyberSWITCH within its group.

SQL SETUP UTILITY

OVERVIEW

A Microsoft SQL Server must be configured for SFVRA Connection Manager system. For best performance, we advise that you install the SQL Server on the same Windows NT machine as the SFVRA Service program. The SQL Server should be set up with SFVRA as the name, SFVRA as the Login ID and use c:\Program Files\SFVRA\SFVRA.SQL to create tables in the SFVRA database. The following instructions are for the SQL Setup Utility written for the ease of configuring your SQL Server.

CONFIGURING THE SQL SERVICE FOR SFVRA-CONN

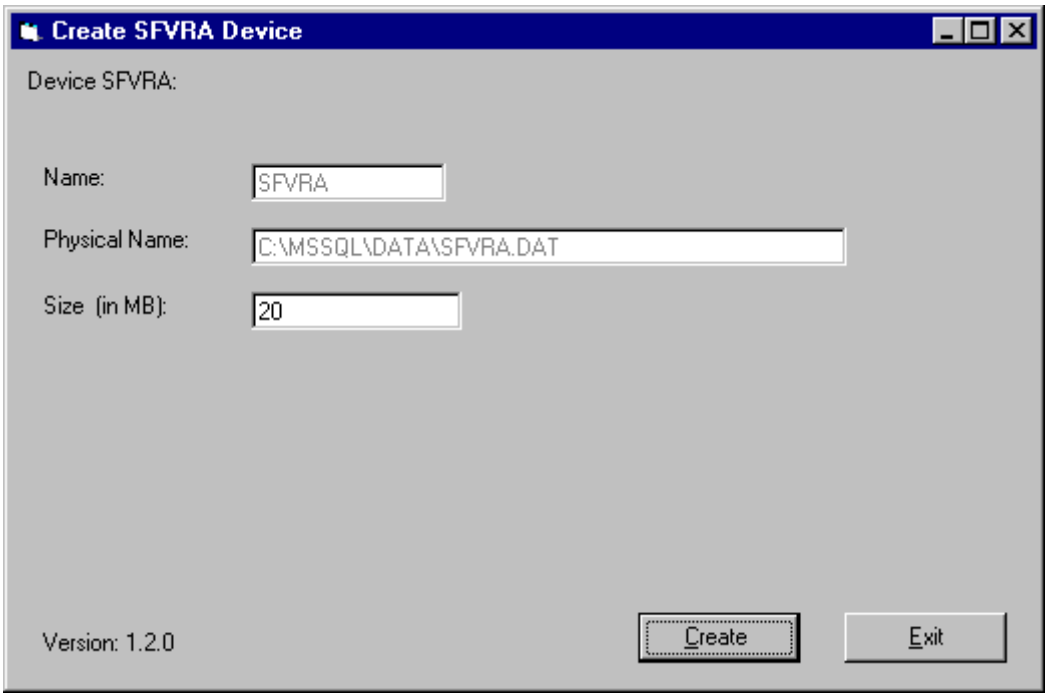
1. From the Start menu\Programs\SFVRA, select *SQL Setup*.

2. Enter the Login ID *sa* and a password, if necessary, and click *OK*. The SQL Setup program executes.

   Note: The "sa" account is the only account that may run the SQL Setup utility. Refer to the *Manage Logins* chapter for more details.

3. The SQL Setup Utility informs you of the processes it will accomplish. Click *Continue.*

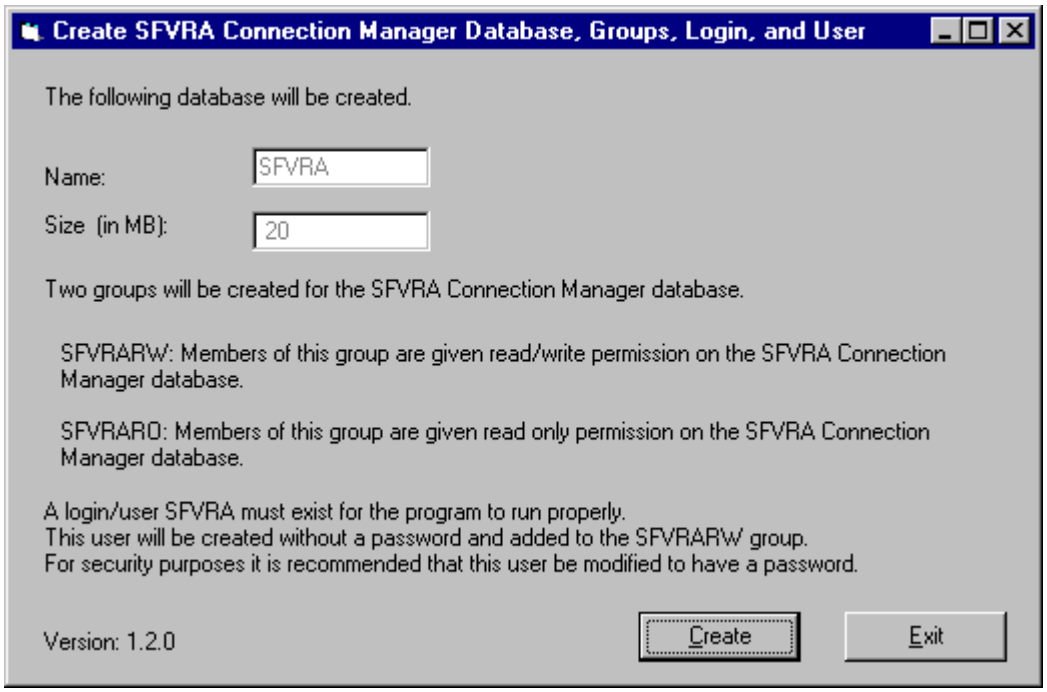
4. The SQL Setup program first creates the SFVRA Device. The following screen appears:



We recommend specifying the device size of at least 20 MB. Click *Create.*

Note: If you want the Device to reside in a different place than indicated by the dialog, you must create the Device in the desired directory before running this application. Refer to the *SQL Server Administrator's Companion* for information on creating the Device. Otherwise, *sfvra.dat* will be created in the same directory as *master.dat*.

5. Once the SFVRA Device has been created, the SQL Setup will create the SFVRA database, groups, login and users. The following screen appears:

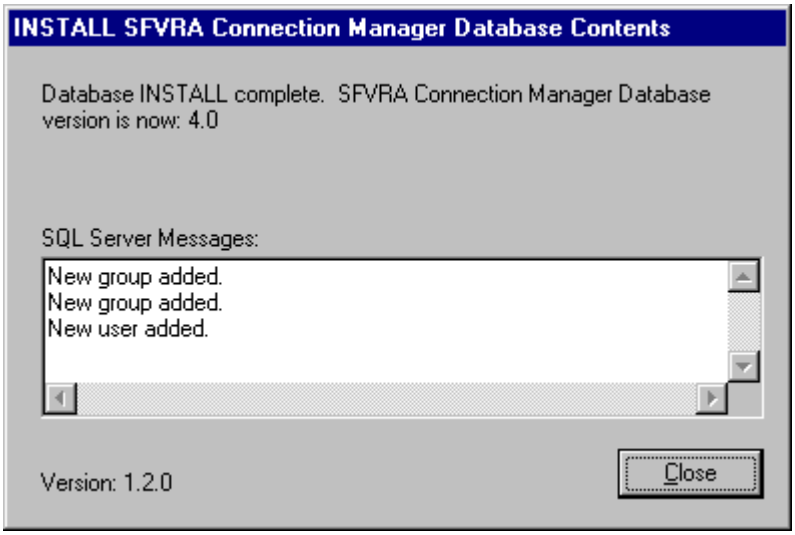

Create SFVRA Connection Manager Database, Groups, Login, and User
The following database will be created.
Name:
SFVRA
Size (in MB):
20
Two groups will be created for the SFVRA Connection Manager database.
SFVRARW: Members of this group are given read/write permission on the SFVRA Connection Manager database.
SFVRARO: Members of this group are given read only permission on the SFVRA Connection Manager database.
A login/user SFVRA must exist for the program to run properly.
This user will be created without a password and added to the SFVRARW group.
For security purposes it is recommended that this user be modified to have a password.
Version: 1.2.0
Create
Exit

Click *Create*.

Note: If you receive an error message stating that the SQL Setup was unable to increase the size of the tempdb database, make a note of it and click *OK*.

6. After the SFVRA Database has been successfully created, the SQL Setup will create database tables. Click *OK*. This procedure may take several minutes, since the SQL Setup runs an ISQL script.

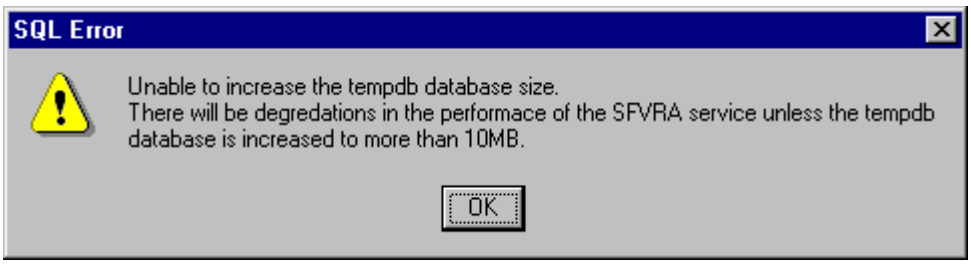
7. When the SQL Setup program has finished, the following screen will be displayed.


INSTALL SFVRA Connection Manager Database Contents
Database INSTALL complete. SFVRA Connection Manager Database version is now: 4.0
SQL Server Messages:
New group added.
New group added.
New user added.
Version: 1.2.0
Close

Ensure that no error messages are listed in the *SQL Server Messages* dialog. Click *Close.*

EXPANDING THE SIZE OF TEMPDB

If you received the following message during the SQL Setup, proceed with the steps outlined below.


SQL Error
Unable to increase the tempdb database size.
There will be degredations in the performace of the SFVRA service unless the tempdb database is increased to more than 10MB.
OK

1. Run the SQL Enterprise Manager.
2. On the Server Manager dialog, select the server that runs the SFVRA database.
3. From the *Manage* menu, select *Database Devices.*
4. Select *master* and click the *Edit Device* icon.
5. Increase the size of the master database to allow for the space required by the tempdb database. Click *Change Now*.
6. From the *Manage* menu, select *Database.*
7. Select *tempdb* from the list of databases, and click the *Edit Database* icon.

8. On the *Database* tab, click *Expand*.

9. Select *master* as the *Database Device* to determine where tempdb should take available space.

10. The default size is the unused space that was just created in master, however you may change the size to fit the needs of tempdb. We recommend that the size of tempdb be at least 9 MB. Click *Expand Now*.

11. Click *OK*.

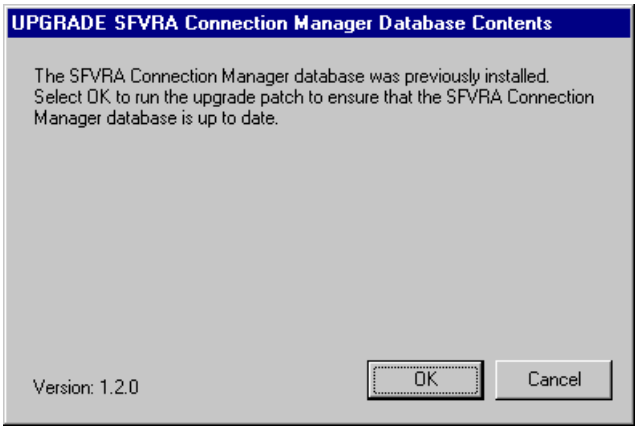
12. Exit SQL Enterprise Manager.

UPGRADING THE SQL SERVICE FOR SFVRA-CONN

1. From the Start menu\Programs\SFVRA, select *SQL Setup*.

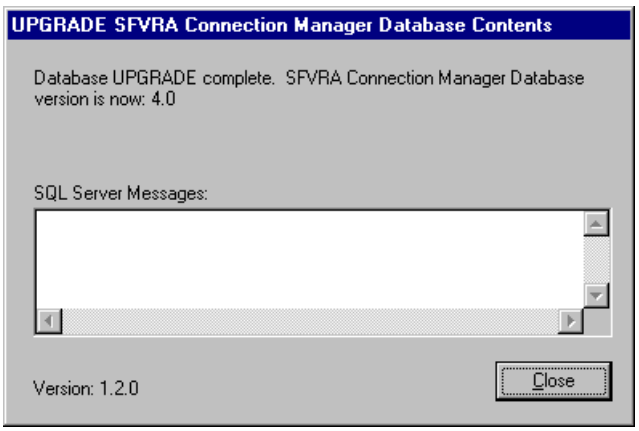
2. Enter the Login ID *sa* and a password, if necessary, and click *OK*. The SQL Setup program executes.

3. The SQL Server Setup Utility first locates the SFVRA database. The following screen appears:


UPGRADE SFVRA Connection Manager Database Contents
The SFVRA Connection Manager database was previously installed.
Select OK to run the upgrade patch to ensure that the SFVRA Connection Manager database is up to date.
Version: 1.2.0
OK
Cancel

4. Click *OK* to upgrade the database.

5. When the upgrade procedure is complete, the following screen appears:


UPGRADE SFVRA Connection Manager Database Contents
Database UPGRADE complete. SFVRA Connection Manager Database version is now: 4.0
SQL Server Messages:
Version: 1.2.0
Close

   Ensure that no errors occurred. Scroll through the list of SQL Server Messages, if any.

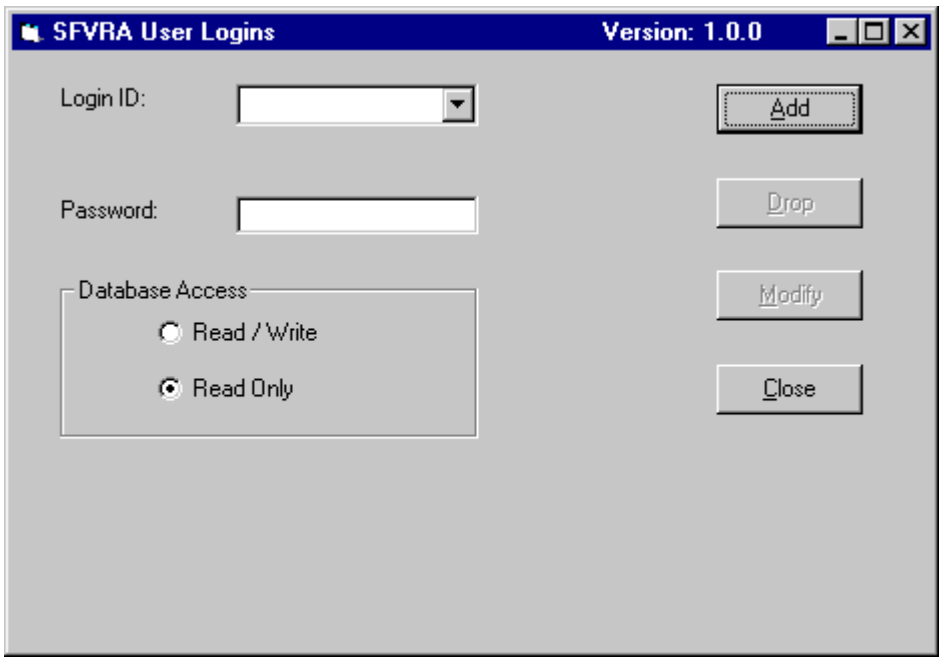
6. Click *Close*.

MANAGE LOGINS

OVERVIEW

There are three types of login accounts for SFVRA Connection Manager. The login ID “sa” is defined by the MS SQL Server for the system administrator. This account has complete access over SFVRA-CONN and all its applications. It is required to run the SQL Setup application and the Manage Logins application. SFVRARW is another type of login ID that has read / write privileges. The login ID “SFVRA“ has read / write privileges and is defined by the SQL Setup application. Additional accounts with read / write privileges can be created using the Manage Logins application. For instance, your Help Desk Manager may need to be able to create new users or to reset a users call usage for a particular month. Lastly, SFVRARO is a type of login ID that has read only privileges. This type could be used for general Help Desk personnel to have Read capabilities only, so that they can review the Current Connection, Connect History, and Problem Log tables, but not have the ability to make changes to a user’s account or see their passwords. The Manage Logins application allows you to create different Login ID’s with different access privileges. Passwords are created and assigned at the administrator’s discretion.

In order to add new accounts or modify existing accounts, you must log in as sa, system administrator of the SQL Server. All other accounts only have the ability to view the Database Access status of the other accounts. The Login ID “SFVRA” is created when the SFVRA Connection Manager software is installed. This account is created with Read / Write access and with no password. We recommend that a password is configured for this account, and any accounts created thereafter.



LOGIN NAME
The Login ID of the account.

PASSWORD
The Password of the account.

DATABASE ACCESS
Determines the type of access for the account.

- Read / Write gives the account the rights to make changes within the Client interface. This does not provide the ability to add new accounts or modify existing accounts, including their own.
- Read Only allows the account only the ability to view the information provided on the Client interface.

Note: The Microsoft SQL Server must be 6.5 or later to configure Read Only access.

CREATING LOGIN ACCOUNTS FOR CLIENTS

1. From the Start menu \ Programs \ SFVRA, select *Manage Logins*.

2. Enter the Login ID *sa* and a password, if necessary, and click *OK*. The Manage Logins program executes.

   Note: The "sa" account is the only account that may make changes to the login accounts. However, read / write and read only accounts may view the access privileges of any account.

3. Select the Login name of the account you wish to modify, or select <*New Login*> to create a new account.

4. Configure a password. You will be prompted to confirm the password when the account is added or modified.

5. Select the type of *Database Access.*

6. Click *Add* for new accounts, or click *Modify* for previously existing accounts. *Drop* removes the account from the database.

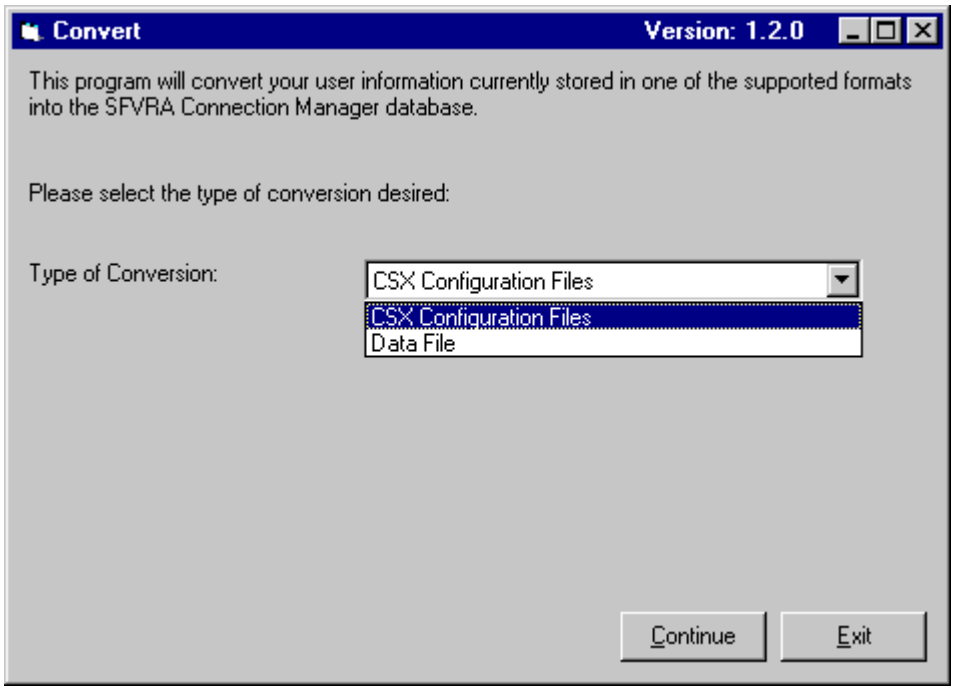
7. Click *Close*.

CONVERT

OVERVIEW

Convert allows the network administrator to translate user information from several formats into the SFVRA Connection Manager database file. Convert reads in the data and adds each user sequentially into the database. If the application encounters a statement that it doesn't recognize, the conversion process will exit and an error message is shown that describes where the error can be found. Once the error is corrected, you can re-run Convert. Convert will not update previously existing users even if changes have been made. The files must be copied to the Windows NT machine where the database resides, or to a network that the NT machine can access.

Note: If convert encounters a user name that already exists in the SFVRA Database, the user will be skipped, regardless if any other information is different. Ensure that all users have unique names.


Convert
Version: 1.2.0
This program will convert your user information currently stored in one of the supported formats into the SFVRA Connection Manager database.
Please select the type of conversion desired:
Type of Conversion:
CSX Configuration Files
CSX Configuration Files
Data File
Continue
Exit

TYPE OF CONVERSION

There are two types of conversion that Convert performs: CSX Configuration Files and Data Files. The CSX configuration files are IP.NEI and, depending on what version of UAA software the CyberSWITCH is running, NETWORK.NEI or DEVDB.NEI. A data file contains only the user's name, password, and IP address.

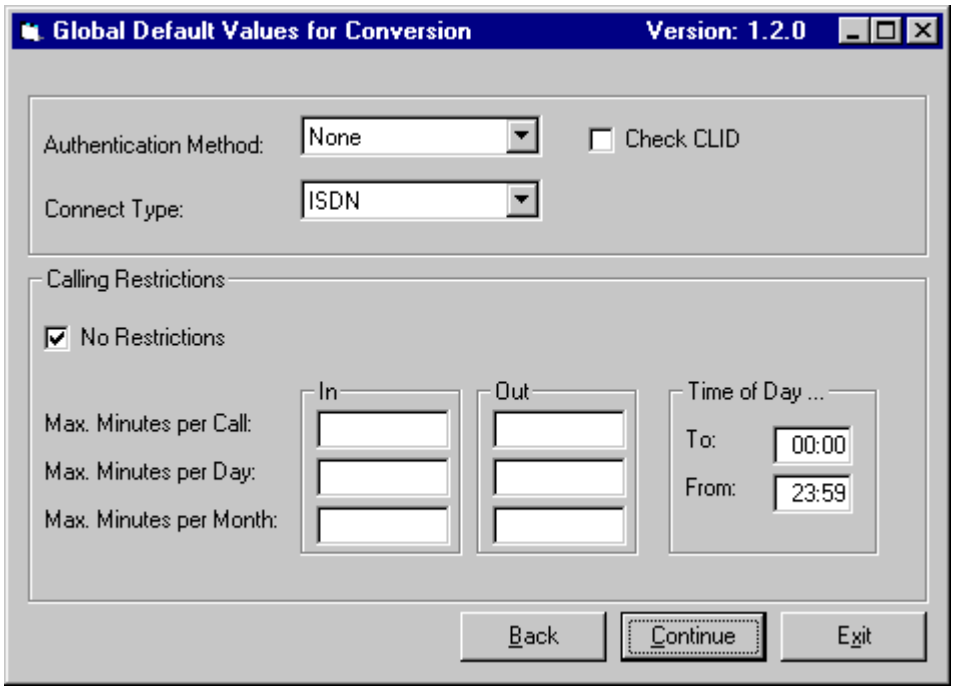
The following is a list of supported file formats that can be translated by Convert:

- CyberSWITCH configuration files
- Data files

CyberSWITCH Configuration Files

The first type are system files for the CyberSWITCH. Convert uses two of these files: IP.NEI and NETWORK.NEI or DEVDB.NEI, depending upon which version of UAA software installed on the CyberSWITCH. The IP.NEI file contains static route information. A static route will be added to the SFVRA database for any user that is named as the next hop. The NETWORK.NEI file or the DEVDB.NEI file contain the information needed for each user, such as protocol, dial out phone number and passwords. These files are located in the \CONFIG directory on the CyberSWITCH.

Although you must select a global authentication method and connect type, Convert will retain all other information for users with different values. For example, if the CyberSWITCH has both ISDN users and Digital Modem users, select the connect type that makes up the majority of users. If you selected ISDN as the connect type, you will need to open the Client interface or run an SQL script to reconfigure the Digital Modem users back to the proper connect type. Since Call Restrictions is implemented on a system wide basis on each CyberSWITCH, Convert only allows a global default value for all users.



Authentication Method

For device level authentication methods, the choices are PAP, CHAP, CLID, CPP, NT, or none.

Connect Type

The type of connection that is to be made when the Remote Access Switch attempts to connect to this user. This feature only affects outbound calls. Users are able to call CyberSWITCH systems using a different protocol. Available connection types are:

- ISDN
- Dedicated
- Digital Modem

CHECK CLID
Validates the Calling Line information received when an ISDN connection is made. The system will compare the incoming Calling Line ID with the value configured (if any) in the User List. If the numbers are identical the connection will be established. Otherwise, the system will reject the incoming call.

When the Calling Line ID security is enabled, entering a Calling Line ID for each remote user is optional. When two remote devices share the same line (a single point-multipoint ISDN line), they can also configure the same Calling Line IDs if they both also have some other type of authentication configured (for example, PAP, CHAP, NT Authentication, or CPP Authentication).

NO RESTRICTIONS
Defines the user to have no restriction on the time of day that calls are made, the length of any particular call, or the maximum minutes per day or month. No Restrictions is enabled as the default.

MAX. MINUTES PER CALL
The maximum amount of time (in minutes) that an inbound or an outbound call is allowed to be active. The default value is 0 minutes. Statistics will be kept to track the total number of call minutes made per call. Existing calls that have surpassed the maximum minutes per call will be disconnected.

MAX. MINUTES PER DAY
The limit of number of inbound or outbound call minutes per day. The default value is 0 call minutes per day. Statistics will be kept to track the total number of call minutes made per day. Existing calls that have surpassed the maximum minutes per day will be disconnected, and no more calls from this user will be accepted until the next day, unless the administrator resets this user's restrictions.

MAXIMUM MINUTES PER MONTH
The maximum number of inbound or outbound call minutes per month. The default value is 0 call minutes per month. Statistics will be kept to track the total number of call minutes made per month. Existing calls that have surpassed the maximum minutes per month will be disconnected and no more calls from this user will be accepted until the next month, unless the administrator resets this user's restrictions.

TIME OF DAY
The allowable hours for outbound calls (there are no time of day restrictions for inbound calls). Calls attempted outside of this time frame will be rejected. Calls that originated within this time frame, but extend outside of the limits will be disconnected. Selecting a "From" value of 00:00 and a "To" value of 00:00 allows the user access during any time of day.

PATH OF .NEI FILES
The .NEI files must be transferred to the Windows NT machine that the SFVRA database resides or on a network that the NT machine has access, and both files must be placed in the same directory. The path of the files merely points to the directory and not the files themselves. Valid for CSX configuration file conversion.

TRANSFERRING .NEI FILES

1. Configure the Windows NT machine or CyberSWITCH so that they are on the same LAN.
2. Connect the two machines with a 10Base-T crossover cable.
3. Start a DOS prompt.
4. Ping the CyberSWITCH to ensure connectivity. For example, if the CyberSWITCH system's LAN address is 134.141.131.1, type:

```
ping 134.141.131.1
```

5. Use a TFTP client application to GET the files from the CyberSWITCH to the Windows NT machine. Or, use the DOS command TFTP <CSX IP Address> GET <source> <destination>. For example, to transfer the IP.NEI file to the C:\TEMP directory on the Windows NT machine, type:

```
tftp 134.141.131.1 get \config\ip.nei c:\temp\ip.nei
```

Note: If the CyberSWITCH system is running a version of UAA software previous to 7.1, the NETWORK.NEI file should be transferred. If the CyberSWITCH is running 7.1 or later software, the DEVDB.NEI file should be transferred.

CONVERTING CSX CONFIGURATION FILES

1. From the Start menu\Programs\SFVRA, select *Convert*. The Convert program executes.
2. Enter a Login ID and a password, if necessary, and click *OK*.

   Note: You must have read/write privileges to run the Convert application. Refer to the *Manage Logins* chapter for more details.

3. Select *CSX Configuration Files* as the file type for conversion. Click *Continue.*
4. Configure any global defaults desired. Click *Continue*.
5. Locate the path of the .NEI files. Click *Finish.*

DATA FILES

The second type is a data file, containing only a name and password or name, password, and IP address. The password is copied to both the PAP/Ethernet Password and the CHAP Secret fields in the SFVRA Database. The data file can be space and tab delineated, and must be in the following format:

```
[user_name]<tab or space>[password]<tab or space>[IP address]
```

Therefore user names that contain spaces will be processed incorrectly. For example, consider the following entry:

```
John<space>Smith<tab>  sesame<tab>    1.1.1.1
```

"John" is processed as the user name, "Smith" is processed as the password, and "sesame" is processed as the IP address. Convert will accept sesame for the IP address. However, once the user is selected in the Client interface and changes have been made, an invalid IP address error will occur when the user is saved to the database.

Note: The IP address is optional.

AUTHENTICATION METHOD
For device level authentication methods, the choices are PAP, CHAP, CLID, CPP, NT, or none.

FILE NAME, INCLUDING PATH, OF THE DATA FILE
The Data File must be transferred to the Windows NT machine that the SFVRA database resides or on a network that the NT machine has access. Include the path and file name of the Data File. Valid for data file conversion.

CONVERTING A DATA FILE

1. From the Start menu\Programs\SFVRA, select *Convert*. The Convert program executes.
2. Enter a Login ID and a password, if necessary, and click *OK*.

   Note: You must have read/write privileges to run the Convert application. Refer to the *Manage Logins* chapter for more details.
3. Select *Data File* as the file type for conversion. Click *Continue.*
4. Select an authentication protocol if desired. Click *Continue*.
5. Locate the path and filename of the data file. Click *Finish.*

CONVERT SYSTEM MESSAGES

The Convert system messages are divided into four types: error, warning, informational and interrogative. These messages have the title *Convert: <Number>*. The type of message is indicated by the number and by different symbols on the dialog box. Messages are numbered using the following scheme:

Error Messages:	1000-1999
Warning Messages:	2000-2999
Informational Messages:	3000-3999
Interrogative Messages:	4000-4999

Each message is listed individually, grouped by type, and listed by number with suggested actions to take in the event of an error.

Other messages that you may encounter are SQL errors and are numbered by the SQL manufacturer. These numbers have the prefix RDO (Remote Data Object). Refer to the *SQL Error Messages* section of the Client *System Messages* chapter for more detail.

ERROR MESSAGES

Error messages signal that a procedure failed. These messages are indicated by on the dialog box and contain a description of each error message and suggestions for a resolution.

Convert: 1000 A Login ID must be entered.
The login operation failed because no Login ID was provided. Check with your system administrator to get the proper Login ID.

Convert: 1001 This version of the SFVRA CONVERT requires SFVRA database version: <version> or later. The current SFVRA database version is: <current_version>. Cannot get the system information for the About form.
The Convert application requires the SFVRA database version to be the same or later. This error occurs when Convert has been upgraded and the database has not. If the Client interface has a later version than the database, Convert will connect to the database, but you will be unable to view or change any information. We recommend that you upgrade the SFVRA database before upgrading the Convert application to avoid this error.

Convert: 1002 System Information is unavailable at this time.
The User Data Source is not defined as a valid user of a trusted SQL server connection, or the connection to the SQL Server has been dropped since the last action. Ensure under the Control Panel, 32-bit ODBC, that the User Data Source for "SFVRA" does not have the "Use Trusted Connection" box checked, or that the server allows this user with a Trusted Connection.

Convert: 1003 This program is available to members of the SFVRARW group only.
Client users that have read only access are unable to run the Convert application. Ensure that your access rights are accurate with the system administrator.

Convert: 1004 The NETWORK.NEI File or DEVDB.NEI File cannot be opened. Check to see you have specified the correct path.
Convert was unable to locate the NETWORK.NEI file or DEVDB.NEI file, depending on the version of UAA software on the CyberSWITCH. Ensure that the specified path and file name is correct.

Convert: 1005 The IP.NEI File cannot be opened. Check to see you have specified the correct path and file name.
Convert was unable to locate the IP.NEI file. Ensure that the specified path is correct.

Convert: 1006 The Data File cannot be opened. Check to see you have specified the correct path and file name.
Convert was unable to locate the Data File. Ensure that the specified path and file name are correct.

Convert: 1007 Unknown Token encountered. Failure occurred at User Name: <User Name> Token: <Token>. User Record(s) Processed: <x>. User Record(s) added to the database: <y>.
The Convert application encountered an unknown token in one of the .NEI files. The unknown token specified in the error statement was found in conjunction with the specified user. Ensure that this file is not corrupt and the token names are accurate. This message also indicates the number of

users processed and added to the database. The “x” indicates the number of user names read from the .NEI file by Convert, while “y” represents the number of users actually added to the database.

Convert: 1008 Error adding user to database. Failure occurred at User Name: <User Name>. User Record(s) processed: <x>. User Record(s) added to the Database: <y>.
Indicates that Convert was unable to add a user from the NETWORK.NEI file or the DEVDB.NEI file to the database because it was unable to access the database or the file is corrupt. Ensure that the database is running, and that the LAN is functioning properly, if applicable. The “x” indicates the number of user names read from the .NEI file by Convert, while “y” represents the number of users actually added to the database.

Convert: 1009 Error adding user to database. Failure occurred at User Name: <User Name>. IP Record(s) processed: <x>. IP Record(s) added to the Database: <y>.
Indicates that Convert was unable to add a static route for a user from the IP.NEI file to the database because it was unable to access the database or the file is corrupt. Ensure that the database is running, and that the LAN is functioning properly, if applicable. The “x” indicates the number of user names read from the IP.NEI file by Convert, while the “y” represents the number of static routes actually added to the database.

Convert: 1010 Error adding user to database. Failure occurred at User Name: <User Name>. User Record(s) processed: <x>. User Record(s) added to the Database: <y>.
Indicates that Convert was unable to add a user from the data file to the database because it was unable to access the database or the file is corrupt. Ensure that the database is running, and that the LAN is functioning properly, if applicable. The “x” indicates the number of user names read from the data file by Convert, while “y” represents the number of users actually added to the database.

Convert: 1011 Invalid time format. Enter time in the format “hh:mm.”
Call Restrictions configuration error. The time format is based on a 24 hour clock, where hh stands for 00 to 23 and mm stands for 00 to 60.

Convert: 1012 Error reading data file. Failure occurred at User Name <User Name>.
Indicates that Convert was unable to process the remaining users after <User Name> because it encountered an error. Ensure that the data file is correctly delineated and has not been corrupted.

WARNING MESSAGES

Warning messages signal events that you should investigate. These messages are indicated by on the dialog box, and may be normal during certain network conditions, or they may indicate a problem. The SFVRA Connection Manager should continue to operate after posting a warning message. There are currently no warning messages for the Convert application.

INFORMATIONAL MESSAGES

SFVRA Connection Manager provides several informational messages. The messages are indicated by on the dialog box and contain information mainly pertaining to actions that are a result of an action that the administrator provoked.

Convert: 3000 User List Conversion Complete. User Record(s) Processed: <x>. User Record(s) added to the Database <y>.
Convert successfully completed the conversion of the users from the NETWORK.NEI file, the DEVDB.NEI file, or the data file. The "x" indicates the number of user names read from the .NEI file or the data file by Convert, while "y" represents the number of users actually added to the database. Users that are processed by Convert but not added to the database indicates that the user name is not unique.

Convert: 3001 IP List Conversion Complete. IP Record(s) Processed: <x>. IP Record(s) added to the Database: <y>.
Convert successfully completed the conversion of the IP static route information for the users from the IP.NEI file. The "x" indicates the number of user names read from the IP.NEI file by Convert, while the "y" represents the number of static routes actually added to the database. Only static routes that indicate the user as the next hop are included in the SFVRA Database.

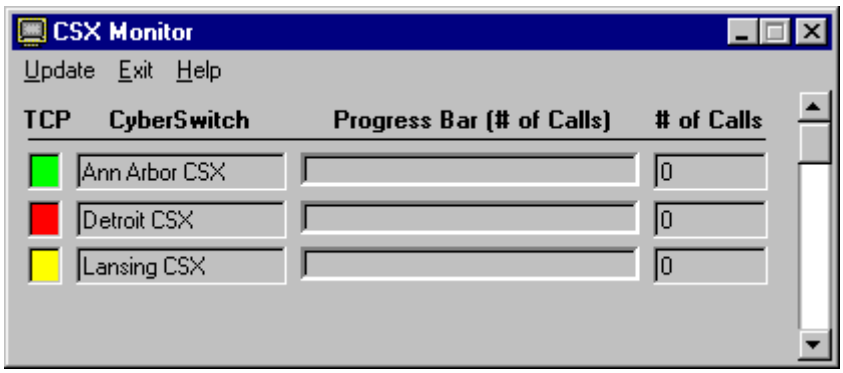
INTERROGATIVE MESSAGES

Interrogative messages provide a last call before performing an action. These messages are indicated by on the dialog box. There are currently no interrogative messages for the Convert application.

CSX MONITOR

OVERVIEW

CSX Monitor allows the network administrator to get a broad view of the TCP connection and the current calls to each CyberSWITCH. The status of each connection is displayed as no TCP/IP connection, waiting - undetected by the SFVRA Service, and TCP/IP connected. When a CyberSWITCH is added to the SFVRA database, CSX Monitor displays the CyberSWITCH within the amount of time indicated in the update cycle. Additionally, the SFVRA Service takes up to three minutes before it recognizes the new CyberSWITCH. However, once the CyberSWITCH is registered in the SFVRA Service, calls are updated up to every 30 seconds plus the amount of time in the update cycle. The update cycle can be specified as 10 seconds, 30 seconds, or 60 seconds.



TCP
Indicates the current state of the TCP/IP connection between the CyberSWITCH and SFVRA-CONN. Each color represents a different TCP state.

- Red indicates that the SFVRA Service recognizes the CyberSWITCH in the database, but there is currently no TCP/IP connection between the CyberSWITCH and SFVRA-CONN.
- Yellow indicates that the CyberSWITCH was recently added to the SFVRA database, but the SFVRA Service has detected it yet.
- Green indicates that a TCP/IP connection has been established between the CyberSWITCH and SFVRA-CONN.

CYBERSWITCH
A name used to uniquely identify this CyberSWITCH in the SQL Database.

PROGRESS BAR (# OF CALLS)
Displays a graphical indication of the number of calls currently maintained by the CyberSWITCH. Each block represents up to 2 calls.

OF CALLS
Indicates the exact number of calls currently maintained by the CyberSWITCH.

RUNNING THE CSX MONITOR

1. From the Start menu \ Programs \ SFVRA, select *CSX Monitor*.

2. Enter a Login ID and a password, if necessary, and click *OK*. The CSX Monitor program executes.

   Note: All logins types may run the CSX Monitor application. Refer to the *Manage Logins* chapter for more details.

3. View the TCP connections and current calls to remote users.

4. For each CyberSWITCH with at least one current call, you may view information about the calls.
   a. Place the cursor over the CyberSWITCH name. The cursor changes to an arrow with a question mark.
   b. Click on the CyberSWITCH name. A report containing each remote user name, the current bandwidth, and a call ID appears.
      - To print the report, click .
      - To export the report to a file, click and select the file type.
   c. Click *Close* to return to CSX Monitor

BRIDGING NETWORK EXAMPLE

OVERVIEW

This chapter provides an example of a simple network using remote bridge devices to access remote users. Bridges are formed between each of the LANs to which the remote bridge devices are connected, and the LAN to which the Remote Access Switches administered by SFVRA Connection Manager is connected.

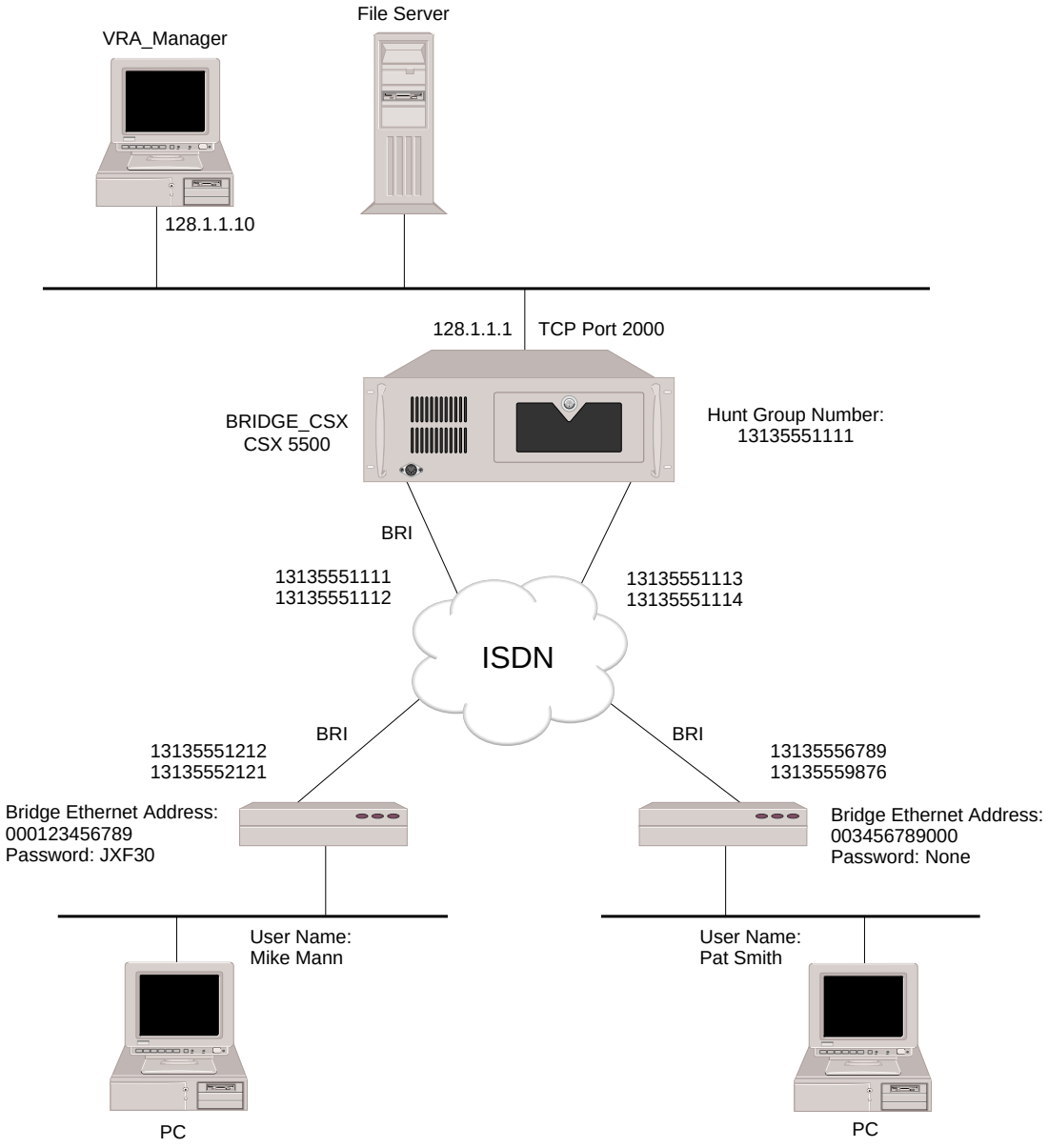
Note that a Hunt Group is used for the BRI lines pictured in Network Topology Worksheet. Remote devices will then only need to configure one telephone number (the Hunt Group number) for the Remote Access Switches instead of all four phone numbers. If the first line is busy, the next line is automatically used, and so on until a free line is found. A Hunt Group number can be arranged through your Service Provider.

INITIAL INSTALLATION STEPS

The first step to configuring a network administered by SFVRA-CONN is to fill out the network worksheets located in the CyberSWITCH documentation. Once you complete the worksheets, you may begin installing SFVRA-CONN. The initial steps are basically the same no matter how complicated the network. Refer to the *System Installation* chapter, which describes in detail each of these steps.

A Network Topology worksheet for this network is included on the following page.

NETWORK TOPOLOGY



SYSTEM DETAILS

CyberSWITCH Name: BRIDGE_CSX
LAN IP Address: 128.1.1.1
TCP Port: 2000
CSX - User Group: REMOTE_BRIDGE

RESOURCES

Type	Slot	Switch Type	Synchronization Type
BRI	*1*	*NI-1*	*N/A*
Ethernet-1	*3*	*N/A*	*N/A*

LINES

BRI Lines

Line Name	Slot	Port	Line Type	Call Screen	TEI	SPID	Directory Number
line1	*1*	*1*	*PPP*		*Auto*	*3135551111*	*13135551111**
						3135551112	*13135551112**
line2	*1*	*2*	*PPP*		*Auto*	*3135551113*	*13135551113**
						3135551114	*13135551114**
				** Hunt Group Number 13135551111*			

BRIDGING

Bridging	***X*** enabled ❒ disabled	
Mode of Operation	❒ restricted ❒ unrestricted	
Bridge Filters		
Bridge Dial Out/ Known Connect List		

CONFIGURE THE CYBERSWITCH

Configure the CyberSWITCH systems according to the procedures in the appropriate documentation. The purpose of this section is not to describe the configuration steps of CyberSWITCH systems, but to point out the areas that are necessary for the users to gain access under control of the SFVRA-CONN.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH SFVRA-CONN

Using CFGEDIT the following information must be configured for a bridging network to be successful:

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add ETHERNET-1 resource, slot 3

Select Options from the Main Menu
- Select IP Routing
  - Enable IP routing. Define the Interface type to be LAN. Enter *128.1.1.1* as the IP Address. Accept the default RIP Receive Control.

Select Security from the Main Menu
- Select Security Level
  - Enable Device Level Security
- Select System Options and Information
  - Enter *BRIDGE_CSX* as the System Name
- Select Device Level Databases
  - Select VRA Manager as the Authentication Database location.
- Select Off-node Server Information
  - Select VRA Manager and configure *2000* for the TCP Port number.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH BRIDGE USERS

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add a BRI resource, include slot and port numbers and switch type
- Select Current Data Lines
  - Add a line, include the name, slot and port numbers, type, and datalinks, if necessary.

Select Options from the Main Menu
- Select MAC Layer Bridging
  - Enable Bridging. All other features are optional and are not directly supported by SFVRA-CONN. This means that they can still be configured, with the noted suggestions, but that the configurations are managed on the CyberSWITCH systems only, and these features should be identical on all CyberSWITCH systems within the same group. Bridge Dial Out and Known Connect List are the exceptions. Since SFVRA-CONN performs the functions of these features, they should not be configured on the individual CyberSWITCH systems.

Note: Security options should not be configured on the CyberSWITCH systems, since SFVRA Connection Manager handles these features.

CONFIGURE THE CYBERSWITCH - USER GROUPING

Note: The SFVRA Connection Manager software should have already been installed, and the Client interface should be activated before proceeding with the following steps.

We will begin the network configuration by defining a CyberSWITCH - User Group. These groups can be used to determine which Remote Access Switches users are allowed to call. In this example, we will configure a group based on the user's protocol. Refer to *Configuring CyberSWITCH - User Groups* for more information.

Note: CyberSWITCH - User Groupings can be used for all types of users, from all areas of your network. In this example, we are grouping users by protocol for ease of understanding the feature only.

1. On the *Tables* menu, select *CyberSWITCH - User Grouping*. The *Table Maintenance* dialog appears.
2. Click *Add*.
3. Enter the name ***REMOTE_BRIDGE***, and click *OK*.
4. Click *Close*.

CONFIGURE THE CYBERSWITCH ON SFVRA-CONN

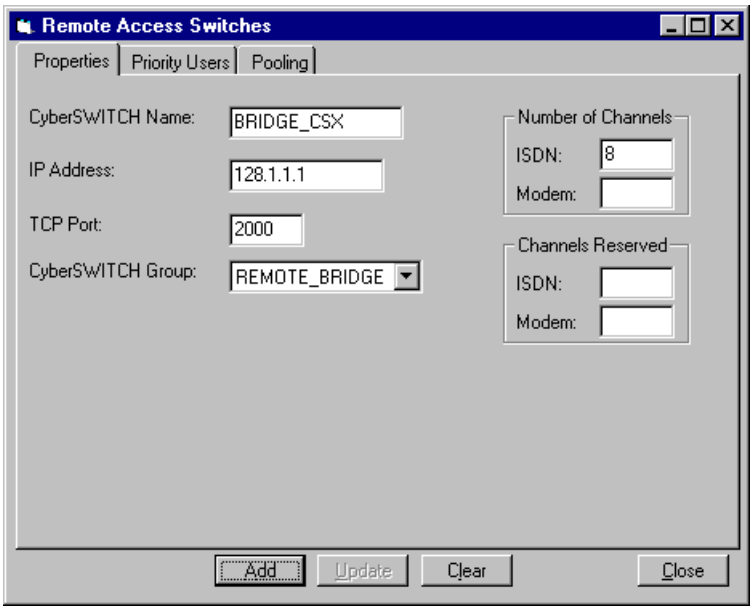
Note: The Client interface should be activated before proceeding with the following steps.

In our example, we only need to supply general properties of the CyberSWITCH in order for SFVRA-CONN to be able to communicate with it. SFVRA-CONN requires a unique name for each CyberSWITCH. It also requires the IP address of the LAN port through which a TCP connection is established to send and receive information. We will also assign the CyberSWITCH to the group that we previously defined. Lastly, in order for the SFVRA-CONN to allow the CyberSWITCH to take incoming calls from users, we must define the number of channels it has available. The Network Topology diagram states that this CyberSWITCH has a BRI resource. For purpose of this example, we will assume that the resource is a BRI-4 adapter. Refer to *Configuring Remote Access Switches* for more information.

1. On the *Functions* menu, select *CyberSWITCH*, or click on the toolbar. The *CyberSWITCH List* dialog appears.
2. Click *Add*. The *Remote Access Switches* dialog appears.

3. Configure CyberSWITCH Properties.

   On the *Properties* tab, enter `BRIDGE_CSX` for the *CyberSWITCH Name*. Enter `128.1.1.1` for the *IP Address*. Enter `2000` for the *TCP Port*. Select `REMOTE_BRIDGE` as the *CyberSWITCH Group*. Enter `8` for the *Number of ISDN Channels*. The *Properties* tab will appear as follows:



4. Click *Add* and then *Close*.

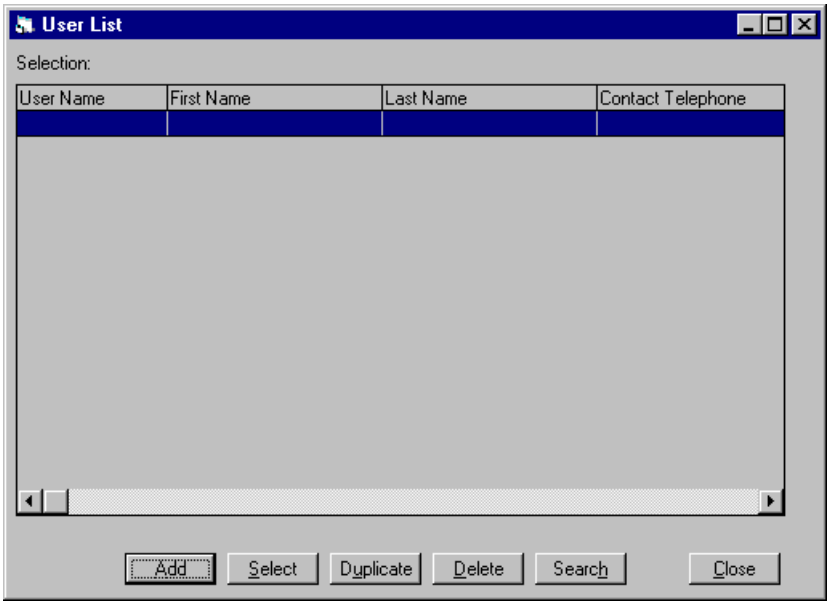
5. Click *Close* on the *CyberSWITCH List* dialog.

CONFIGURE USER RECORDS

Note: The Client interface should be activated before proceeding the following steps.

This network has remote users, and the user information for each of those users must be configured. Each user must have a unique name. These users will be configured without call restrictions. Device level security is used in conjunction with Calling Line ID's.

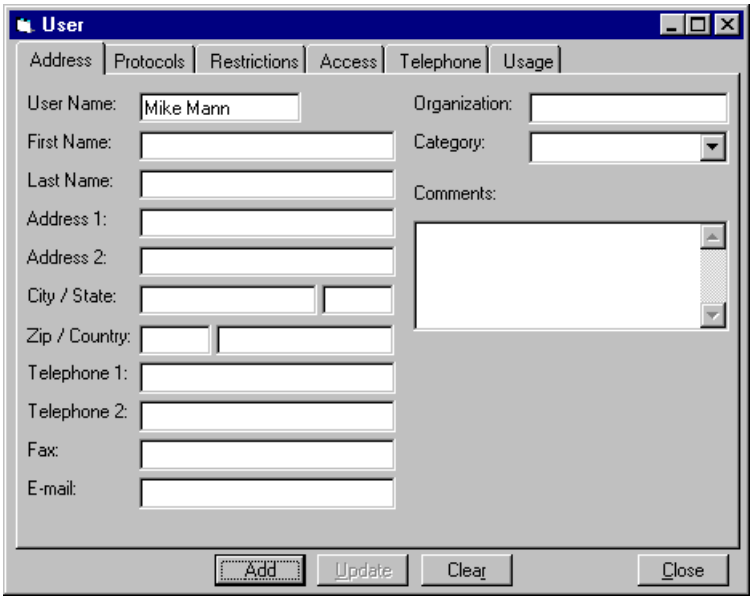
1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog is then displayed as follows:



2. To add remote users, click *Add*. The *User* dialog appears.

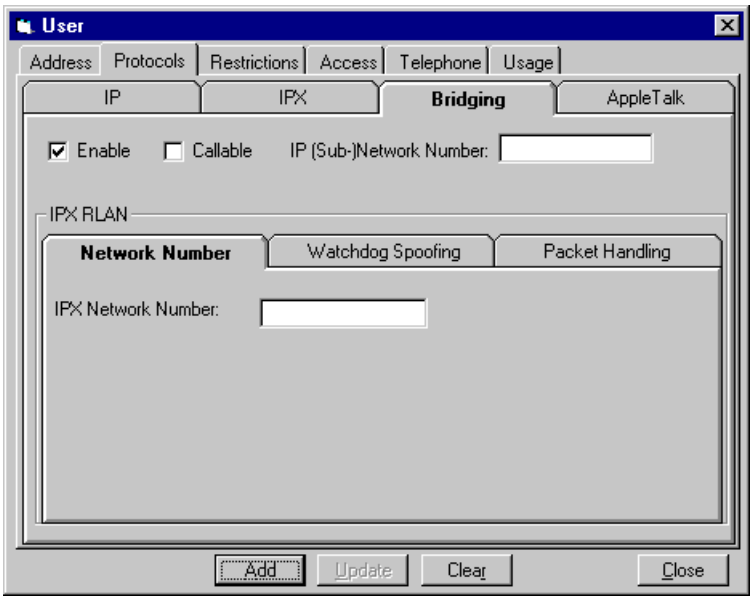
3. Define the User Name.

   For this example, we will configure the user "Mike Mann" first. On the *Address* tab, enter `Mike Mann` for the *User Name*. Only the User Name is required and it must be unique. Other fields are informational for use by the Network Administrator or Help Desk. The *Address* tab should appear as shown below:



4. Enable the Bridging Protocol.

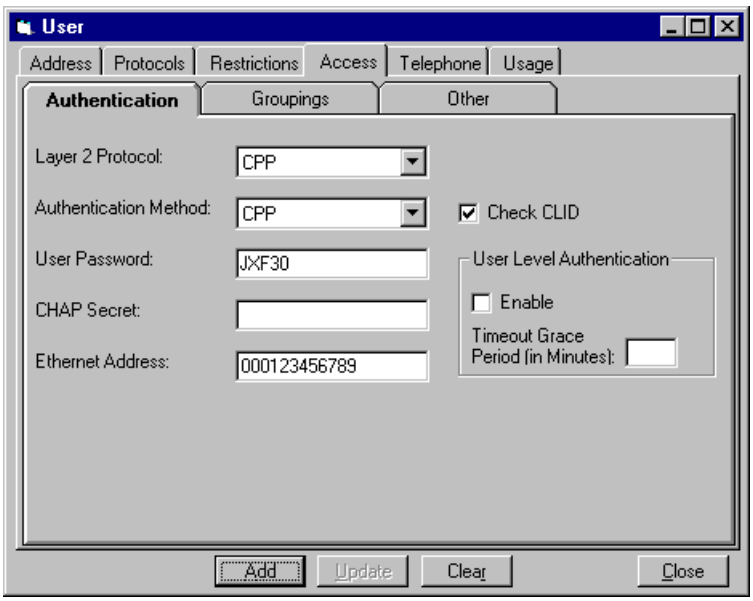
   In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Select *Bridging* on the *Protocols* tab and enter the information as it appears below:



5. On the *Restrictions* tab, accept the default values.

6. Configure Authentication for user “Mike Mann.”

   Select *Authentication* on the *Access* tab. Select ***CPP*** as the *Layer 2 Protocol*. Select ***CPP*** as the *Authentication Method*. In this case, we opt to have security check both the Ethernet address and a password. Enter ***JXF30*** for the *User Password*. Enter ***000123456789*** for the *Ethernet Address*. Enable *Check CLID* for additional security. After the user authentication has been entered, the *Authentication* tab will appear as follows:

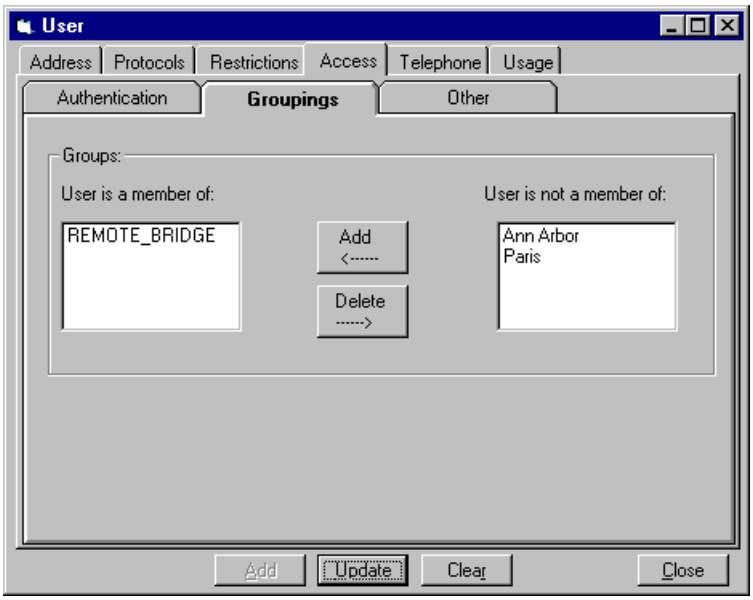


7. Click *Add*.

   Certain user features require the user to be configured in the database before the feature itself can be configured. These features include: configuring static routes, assigning a user to a group, and configuring telephone numbers and Calling Line ID’s. The next parameter that we will configure for user “Mike Mann” is the CyberSWITCH - User Group, therefore we need to add the user to the database first.

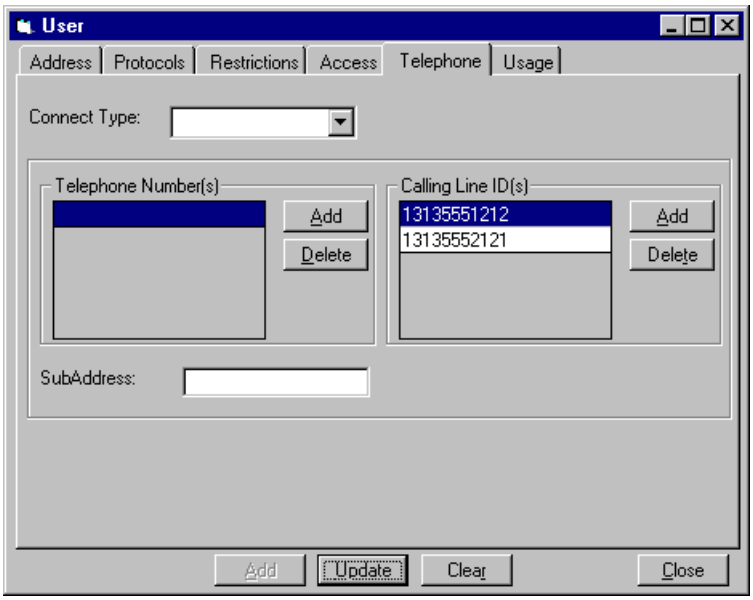
8. Assign the user to a group.

   In order for the user "Mike Mann" to be allowed to connect with the CyberSWITCH "BRIDGE_CSX," the user must be in the same group. Select *Groupings* on the *Access* tab. Select ***REMOTE_BRIDGE*** in the *User is not a member of* box and click *Add*. The *Groupings* tab should appear as shown below:



9. Configure Calling Line ID's.

   Since we enabled *Check CLID* security, we need to configure a Calling Line ID to check. Select the *Telephone* tab. Under Calling Line ID(s), click *Add*, enter ***13135551212***, and click *OK*. Click *Add* again, enter ***13135552121***, and click *OK*. The *Telephone* tab should appear as shown below:



10. Click *Update* and then click *Close.*

11. Click *Close* on the *User List* dialog.

Next enter the user information for Pat Smith. This user is also a CPP bridge, and is configured using the same authentication as user Mike Mann, except we will configure no password for user Pat Smith. Enter 00345678900 for the bridge Ethernet address, 13135556789 for the first calling line ID, and 13135559876 for the second calling line ID. Pat Smith should be added to the REMOTE_BRIDGE group.

VERIFY CONFIGURATIONS

Steps on how to verify the installation are detailed in the *System Verification* chapter. Refer to the *System Verification* chapters of your CyberSWITCH documentation for more specific details on verifying the CyberSWITCH features. This section gives an outline of which steps should be executed.

On the SFVRA-CONN Client:

Check Group assignments

On each system:

Verify resources are operational
Verify WAN Lines Available

IP NETWORK EXAMPLE

OVERVIEW

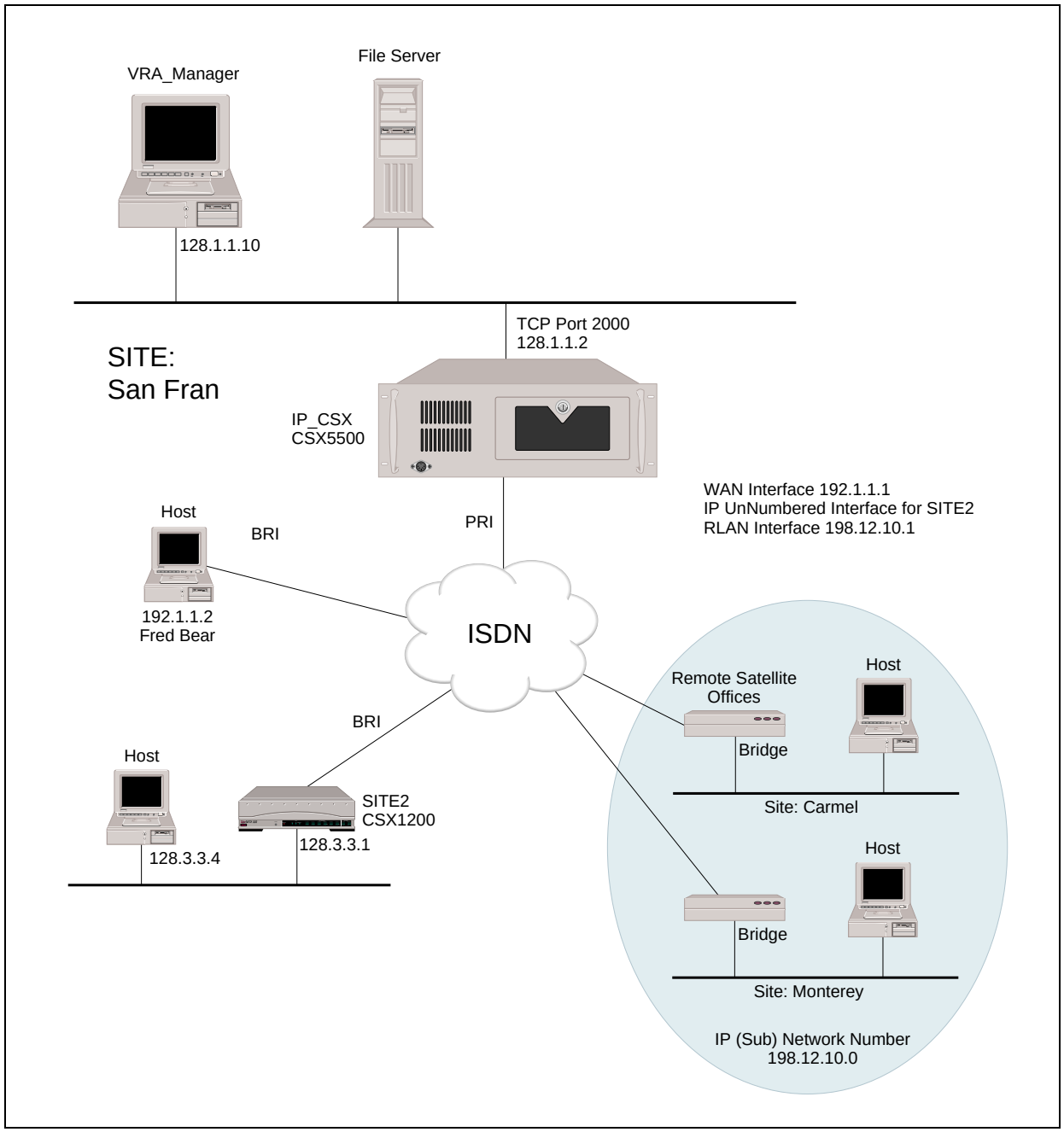
This sample network depicts a company that has an IP network with users accessing the network from their homes, from two satellite offices that have an IP Host that communicates through a Remote Bridge, and from a branch office that communicates through a router that does not support IP RIP. This CyberSWITCH uses a Primary Rate line that can support 23 users at 64Kbps.

INITIAL INSTALLATION STEPS

The first step to configuring a network administered by SFVRA Connection Manager is to fill out the network worksheets located in the CyberSWITCH documentation. Once you complete the worksheets, you may begin installing SFVRA-CONN. The initial steps are basically the same no matter how complicated the network. Refer to the *System Installation* chapter, which describes in detail each of these steps.

A Network Topology worksheet for this network is included on the following page.

NETWORK TOPOLOGY



SYSTEM DETAILS

CyberSWITCH Name: IP_CSX
LAN IP Address 128.1.1.2
TCP Port Number 2000
CSX - User Group IP

RESOURCES

Type	Slot	Switch type	Synchronization type
PRI	***1***	***5ESS***	***slave***
Ethernet-1	***3***		

LINES

PRI Lines

Name	Slot	Port	Framing type	Line coding	Sig. method	Line build-out
Line 1	***1***	***1***	***ESF***	***B8ZS***	***common channel***	***0-35***

IP ROUTING

IP Routing	***X*** enabled ❒ disabled
Mode of Operation	***X*** router ❒ IP host

Network Interface Information

LAN	Name	***San Fran***		
	IP address	***128.1.1.1***		
	Mask	***255.255.0.0***		
Unnumbered WAN	***X*** need ❒ don't need			
Remote LAN	Name	***Satellites***		
	IP address	***198.12.10.1***		
	Mask	***255.255.0.0***		
Traditional WAN	Name	***San Jose***		
	IP address	***192.1.1.1***		
	Mask	***255.255.255.0***		
Direct Host WAN	Name			
	IP address			
	Mask			
IP Host Mode	IP address			
	Mask			

CONFIGURE THE CYBERSWITCH

Configure the CyberSWITCH systems according to the procedures in the appropriate documentation. The purpose of this section is not to describe the configuration steps of CyberSWITCH systems, but to point out the areas that are necessary for the users to gain access under control of the SFVRA-CONN.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH SFVRA-CONN

Using CFGEDIT the following information must be configured for an IP Routing network to be successful:

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add ETHERNET-1 resource, slot 3

Select Options from the Main Menu
- Select IP Routing
  - Enable IP routing. Define an Interface type to be LAN. Enter *128.1.1.2* as the IP Address. Accept the default RIP Receive Control.

Select Security from the Main Menu
- Select Security Level
  - Enable Device Level Security
- Select System Options and Information
  - Enter *IP_CSX* as the System Name
- Select Device Level Databases
  - Select VRA Manager as the Authentication Database location.
- Select Off-node Server Information
  - Select VRA Manager and configure *2000* for the TCP Port number.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH IP USERS

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add a PRI resource, include slot number, switch type and synchronization type.
- Select Current Data Lines
  - Add a line, include the name, slot and port numbers, framing type, line coding, signaling method, and line build out.

Select Options from the Main Menu
- Select IP
  - Enable the IP Protocol. Define the Interface type to be WAN. Enter *192.1.1.1* as the IP Address. Accept the default RIP Receive Control. Define another interface to be WAN (Remote LAN). Enter *198.12.10.1* as the IP Address. Define a third interface as WAN UnNumbered.

Note: Security options should not be configured on the CyberSWITCH systems, since SFVRA Connection Manager handles these features.

CONFIGURE THE CYBERSWITCH - USER GROUPING

Note: The Client interface should be activated before proceeding the following steps.

We will begin the network configuration by defining a CyberSWITCH - User Group. These groups can be used to determine which Remote Access Switches the users are allowed to call. In this example, we will configure a group based on the user's protocol.

Note: CyberSWITCH - User Groupings can be used for all types of users, from all areas of your network. In this example, we are grouping users by protocol for ease of understanding the feature only.

1. On the *Tables* menu, select *CyberSWITCH - User Grouping*. The *Table Maintenance* dialog appears.

2. Click *Add*.

3. Enter the name *IP*, and click *OK*.

4. Click *Close*.

CONFIGURE THE CYBERSWITCH ON SFVRA-CONN

Note: The SFVRA-CONN software should have already been installed, and the Client interface should be activated before proceeding the following steps.

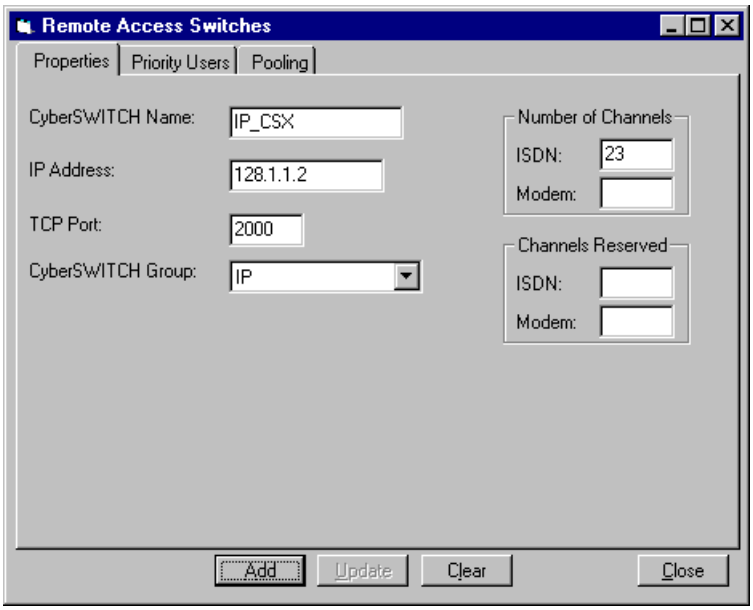
In our example, we only need to supply general properties of the CyberSWITCH in order for SFVRA-CONN to be able to communicate with it. SFVRA-CONN requires a unique name for each CyberSWITCH. It also requires the IP address of the LAN port through which a TCP connection is established to send and receive information. We will also assign the CyberSWITCH to the group that we previously defined. Lastly, in order for the SFVRA-CONN to allow the CyberSWITCH to take incoming calls from users, we must define the number of channels it has available. The Network Topology diagram states that this CyberSWITCH has a PRI line, which indicates that it has 23 channels available for users. Refer to *Configuring Remote Access Switches* for more information.

1. On the *Functions* menu, select *CyberSWITCH*, or click on the toolbar. The *CyberSWITCH List* dialog appears.

2. Click *Add*. The *Remote Access Switches* dialog appears.

3. Configure CyberSWITCH Properties.

   On the *Properties* tab, enter `IP_CSX` for the *CyberSWITCH Name*. Enter `128.1.1.2` for the *IP Address*. Enter `2000` for the *TCP Port*. Select `IP` as the *CyberSWITCH Group*. Enter `23` for the *Number of ISDN Channels*. The *Properties* tab will appear as follows:



4. Click *Add* and then *Close*.

5. Click *Close* on the *CyberSWITCH List* dialog

CONFIGURE USER RECORDS

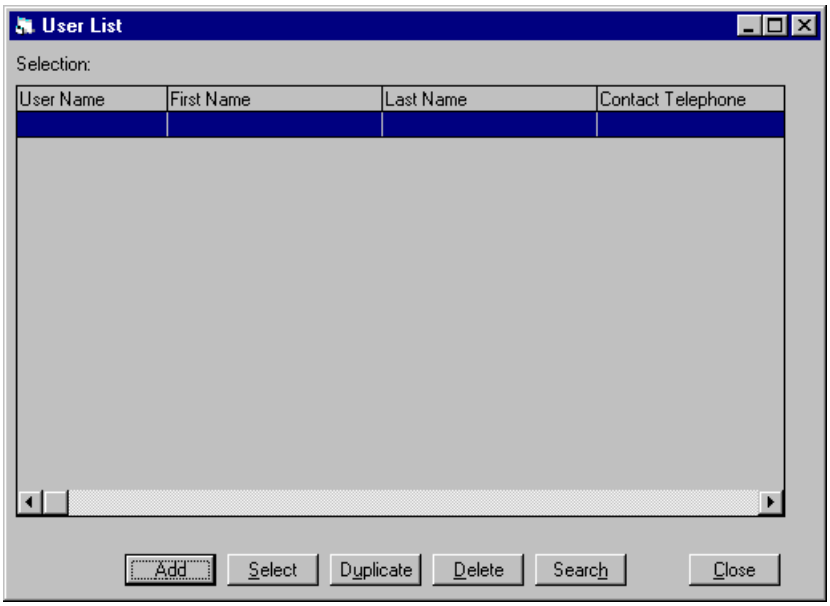
Note: The Client interface should be activated before proceeding the following steps.

In this example, there are three types of IP users, IP WAN, IP WAN with a Remote Bridge Device, and IP WAN with a PPP Device. Using the detailed instructions for these steps found in *Configuring Users*, complete the configuration information indicated in the following procedures.

CONFIGURING IP WAN USERS

The user “Fred Bear” is an IP WAN remote device. This user will be configured without call restrictions or security.

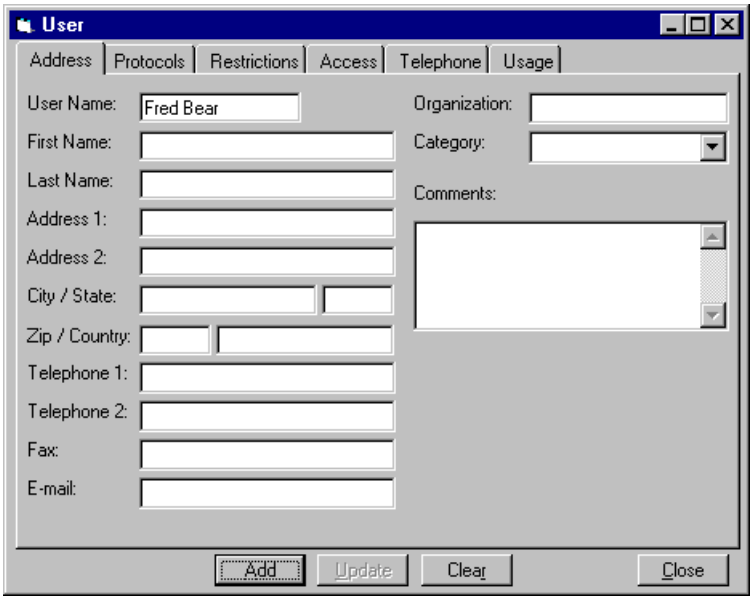
1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog is then displayed as follows:



2. To add remote users, click *Add*. The *User* dialog appears.

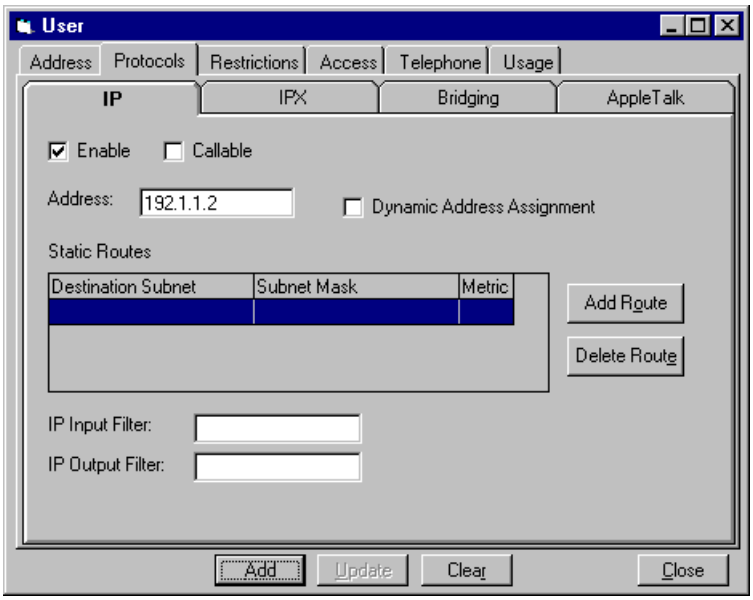
3. Define the User Name.

   For this example, we will configure the user "Fred Bear" first. On the *Address* tab, enter `Fred Bear` for the *User Name*. Only the User Name is required and it must be unique. Other fields are informational for use by the Network Administrator or Help Desk. The *Address* tab should appear as shown below:



4. Enable the IP Protocol.

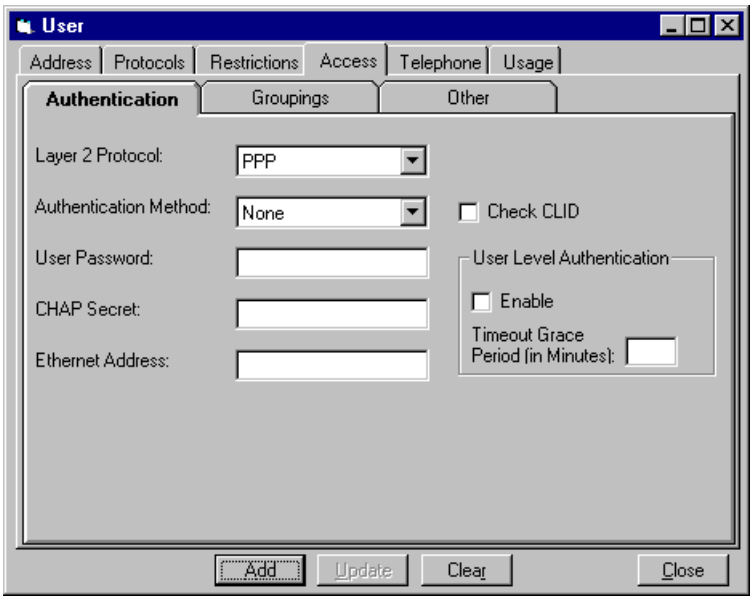
   In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Select *IP* on the *Protocols* tab and enable IP. Enter the *IP Address* `198.12.10.0`.



5. On the *Restrictions* tab, accept the default values.

6. Configure Authentication for user "Fred Bear."

   Select *Authentication* on the *Access* tab. Select *PPP* as the *Layer 2 Protocol*. Select *None* as the *Authentication Method*. After the user authentication has been entered, the *Authentication* tab will appear as follows:

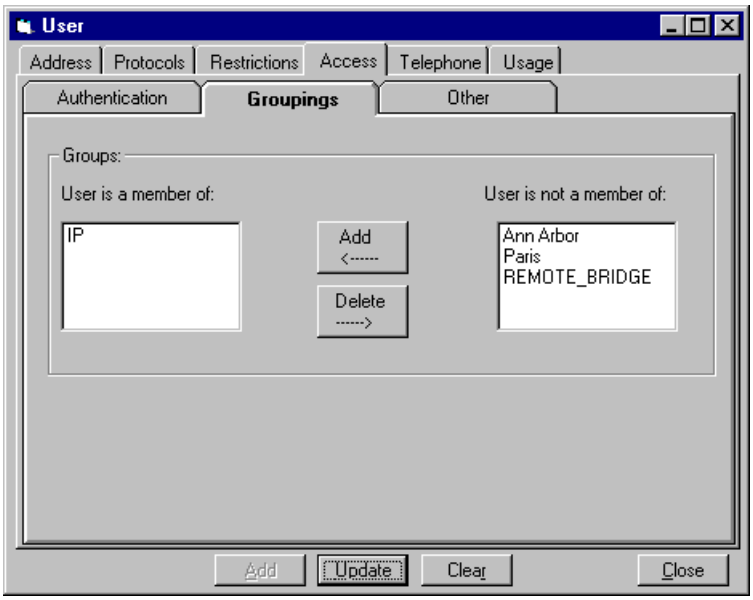


7. Click *Add*.

   Certain user features require the user to be configured in the database before the feature itself can be configured. These feature include: configuring static routes, assigning a user to a group, and configuring telephone numbers and Calling Line ID's. The next parameter that we will configure for user "Fred Bear" is the CyberSWITCH - User Group, therefore we need to add the user to the database first.

8. Assign the user to a group.

   In order for the user "Fred Bear" to be allowed to connect with the CyberSWITCH "IP_CSX," the user must be in the same group. Select *Groupings* on the *Access* tab. Select *IP* in the *User is not a member of* box and click *Add*. The *Groupings* tab should appear as shown below:



9. Click *Update* and then click *Close*.

10. Click *Close* on the *User List* dialog.

CONFIGURING IP WAN USERS WITH REMOTE BRIDGE DEVICES

This sample network has two remote satellite offices in Monterey and Carmel, California that need to be in daily electronic communication with their Corporate Office in San Francisco. Each satellite office has an IP Host that communicates through a Remote Bridge. This example uses a WAN (Remote LAN) Interface to allow the two remote bridge devices to connect to an IP subnet. The CyberSWITCH treats these devices connected to the RLAN network interface as if they were connected to the same Ethernet segment.

Note: This example only provides screen shots that are distinctly different from those in the previous configuration section. If necessary, refer to the example screens in *Configuring IP WAN Users* for more detail.

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

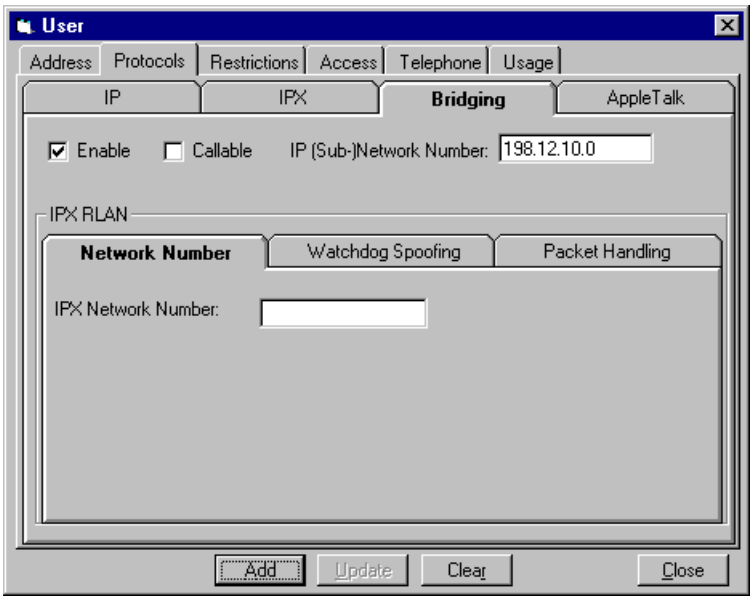
2. To add remote users, click *Add*. The *User* dialog appears.

3. Define the User Name.

   On the *Address* tab, enter `Monterey` for the *User Name*. Only the User Name is required and it must be unique. Other fields are informational for use by the Network Administrator or Help Desk.

4. Enable the Bridging Protocol.

   In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Select *Bridging* on the *Protocols* tab and enable Bridging. Although the user Monterey is a bridge, we need to configure an IP (Sub-) Network Number. Enter the *IP Address* `198.12.10.0`. The *IP* tab should appear as shown below:



5. On the *Restrictions* tab, accept the default values.

6. Configure Authentication for user "Monterey."

   Select *Authentication* on the *Access* tab. Select `PPP` as the *Layer 2 Protocol*. Select `CPP` as the *Authentication Method*. Enter `q3bay` for the *Password*. Enter `123123123123` for the *Ethernet Address*.

7. Click *Add*.

   Certain user features require the user to be configured in the database before the feature itself can be configured. These feature include: configuring static routes, assigning a user to a group, and configuring telephone numbers and Calling Line ID's. The next parameter that we will configure for user "Monterey" is the CyberSWITCH - User Group, therefore we need to add the user to the database first.

8. Assign the user to a group.

   In order for the user "Monterey" to be allowed to connect with the CyberSWITCH "IP_CSX," the user must be in the same group. Select *Groupings* on the *Access* tab. Select `IP` in the *User is not a member of* box and click *Add*.

9. Click *Update* and then click *Close*.

10. Click *Close* on the *User List* dialog.

Next enter the user information for Carmel. This user is also a remote bridge that uses the IP protocol, and is configured using the same authentication as user Monterey, except we will configure dharry as the password for user Carmel. Enter 22222222222 for the bridge Ethernet address. Carmel should be added to the IP group.

CONFIGURING AN IP WAN USER WITH A PPP DEVICE

This sample network uses IP routing to connect two of our products, both using PPP. In this case, we will use an UnNumbered interface.

Note: This example only provides screen shots that are distinctly different from those in the previous configuration section. If necessary, refer to the example screens in *Configuring IP WAN Users* for more detail.

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

2. To add remote users, click *Add*. The *User* dialog appears.

3. Define the User Name.

   On the *Address* tab, enter `SITE2` for the *User Name*. Only the User Name is required and it must be unique. Other fields are informational for use by the Network Administrator or Help Desk.

4. Enable the IP Protocol.

   In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Select *IP* on the *Protocols* tab and enable IP. Enter the *IP Address* `0.0.0.0`.

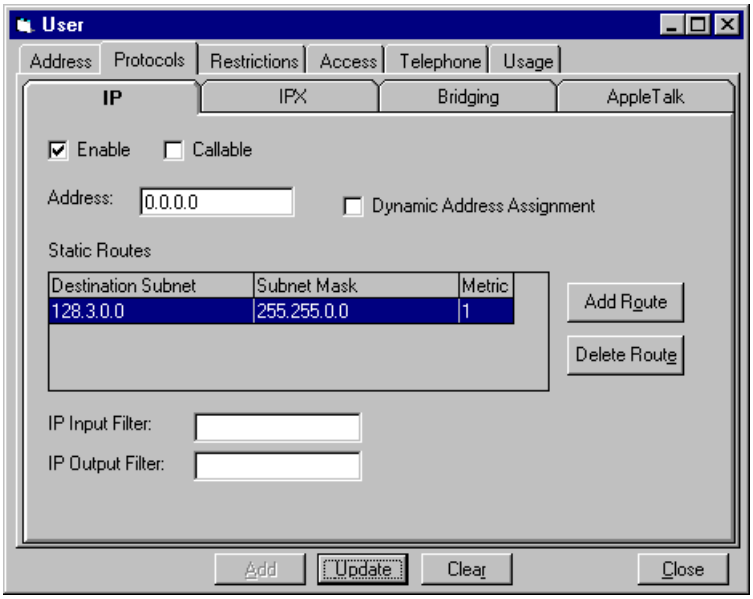
5. Click *Add*.

   Certain user features require the user to be configured in the database before the feature itself can be configured. These feature include: configuring static routes, assigning a user to a group, and configuring telephone numbers and Calling Line ID's. The next parameter that we will configure for user "SITE2" is a static route, therefore we need to add the user to the database first.

6. Configure a static route.

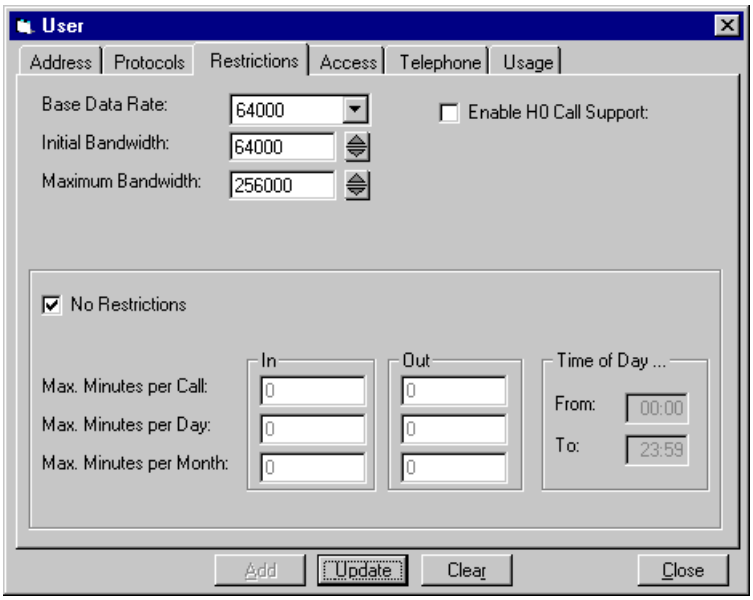
   Select *IP* on the *Protocols* tab. Under *Static Routes*, click *Add Route*. Enter `128.3.0.0` as the *Destination IP Address*, and press the Tab key. Accept the default *Subnet Mask*, and press the Tab key. Enter a *Metric* value of `1`, and click *Add*. The *IP* tab will appears as follows:

   Note: Although "SITE2" is a callable user, the Callable feature can not be enabled until a telephone number is configured. We will refer back to the IP tab later on in this example to enable this feature.



7. Increase the Maximum Bandwidth.

   In this example, user "dallasnet" has no call restrictions and a maximum bandwidth of 256000 bps. Select the *Restrictions* tab and enter the information as it appears below.



8. Configure Authentication for user "Monterey."

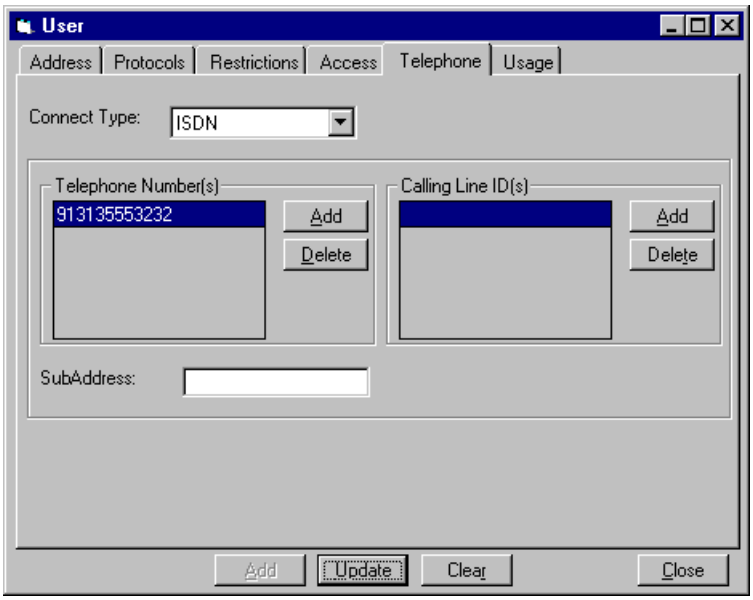
   Select *Authentication* on the *Access* tab. Select ***PPP*** as the *Layer 2 Protocol*. Select ***CHAP*** as the *Authentication Method*. Enter ***ikcd98s*** for the *CHAP Secret*.

9. Assign the user to a group.

   In order for the user "SITE2" to be allowed to connect with the CyberSWITCH "IP_CSX," the user must be in the same group. Select *Groupings* on the *Access* tab. Select ***IP*** in the *User is not a member of* box and click *Add*.

10. Configure a telephone line for central site calls.

    In order for a CyberSWITCH to call user "SITE2," the type of connection needs to be defined and a telephone number for the user must be available. Select the *Telephone* tab. Select *ISDN* as the *Connect Type*. Under *Telephone Number(s)*, click *Add*, enter ***913135553232***, and click *OK*.



11. Configure the user "SITE2" to be callable by the central site.

    Return to *IPX* on the *Protocols* tab. Enable the *Callable* feature.

12. Click *Update* and then click *Close.*

13. Click *Close* on the *User List* dialog.

CONFIGURE NETWORK PROXIES

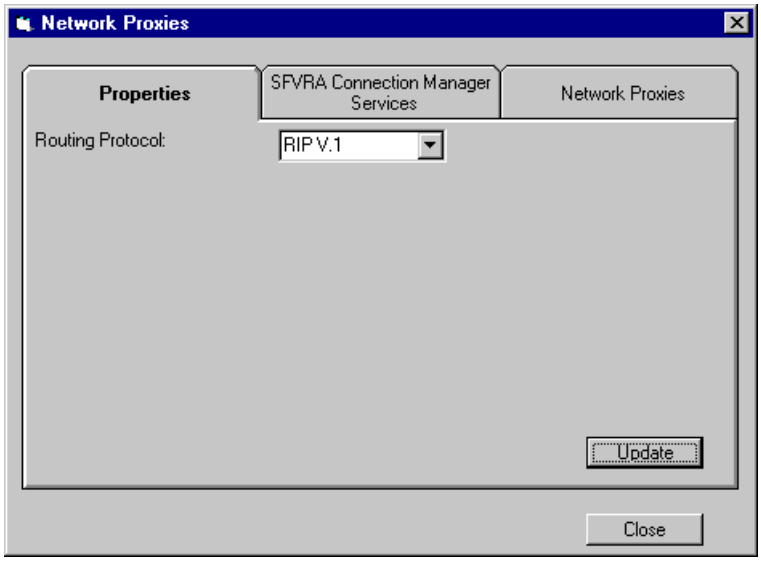
Note: The SFVRA Connection Manager software should have already been installed, and the Client interface should be activated before proceeding the following steps.

Using the detailed instructions for these steps found in *Configuring Network Proxies*, complete the configuration information indicated in the following procedures.

1. On the *Functions* menu, select *Network Proxies*, or click on the toolbar. The *Network Proxies* dialog appears.

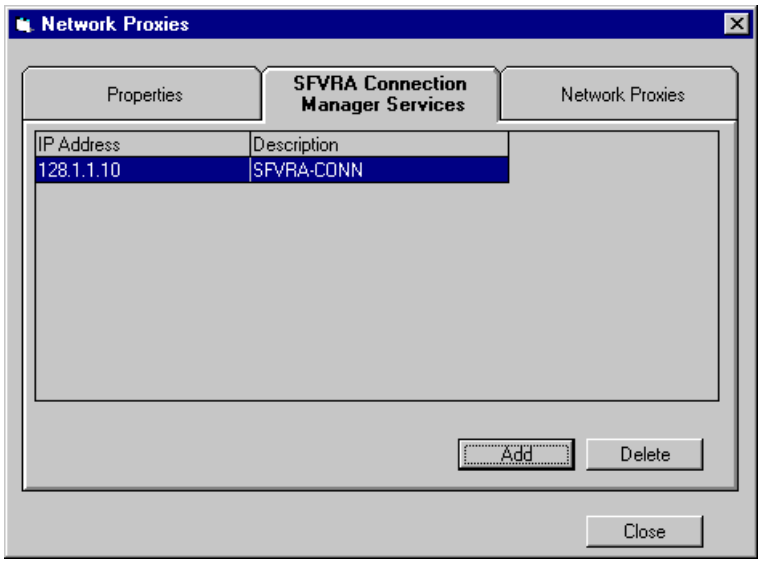
2. Configure basic routing properties.

   On the *Properties* tab, select `RIP V.1` as the *Routing Protocol.*



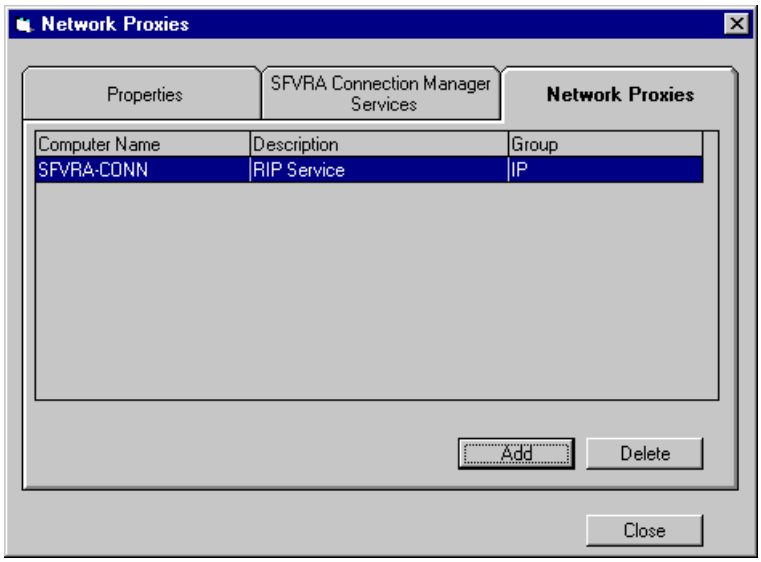
3. Define the location of the SFVRA Service(s).

   Select the *SFVRA Connection Manager Services* tab. Click *Add*. Enter `128.1.1.10` as the *IP Address*. Enter `SFVRA-CONN` for the *Description*. Click *OK*.



4. Assign the RIP Service to a group.

   Select the *Network Proxies* tab. Click *Add*. Enter ***SFVRA_CONN*** for the *Computer Name*. Enter ***RIP Service*** for the *Description*. Select ***IP*** as the *Group*. Click *OK*.



5. Click *Close*.

VERIFY CONFIGURATIONS

Steps on how to verify the installation are detailed in the *System Verification* chapter. Refer to the *System Verification* chapters of your CyberSWITCH documentation for more specific details on verifying the CyberSWITCH features. This section gives an outline of which steps should be executed.

On the SFVRA-CONN Client:

Check Group assignments

On each system:

Verify resources are operational

Verify WAN Lines Available

IPX NETWORK EXAMPLE

OVERVIEW

This sample network uses IPX protocol to allow remote devices and their servers to communicate. It illustrates a master network ("Enterprise LAN") which supports the following:

- a Virtual Ethernet WAN network to communicate with remote bridges (using a Remote LAN interface)
- a traditional WAN network to communicate with a remote IPX router (using a traditional WAN interface).

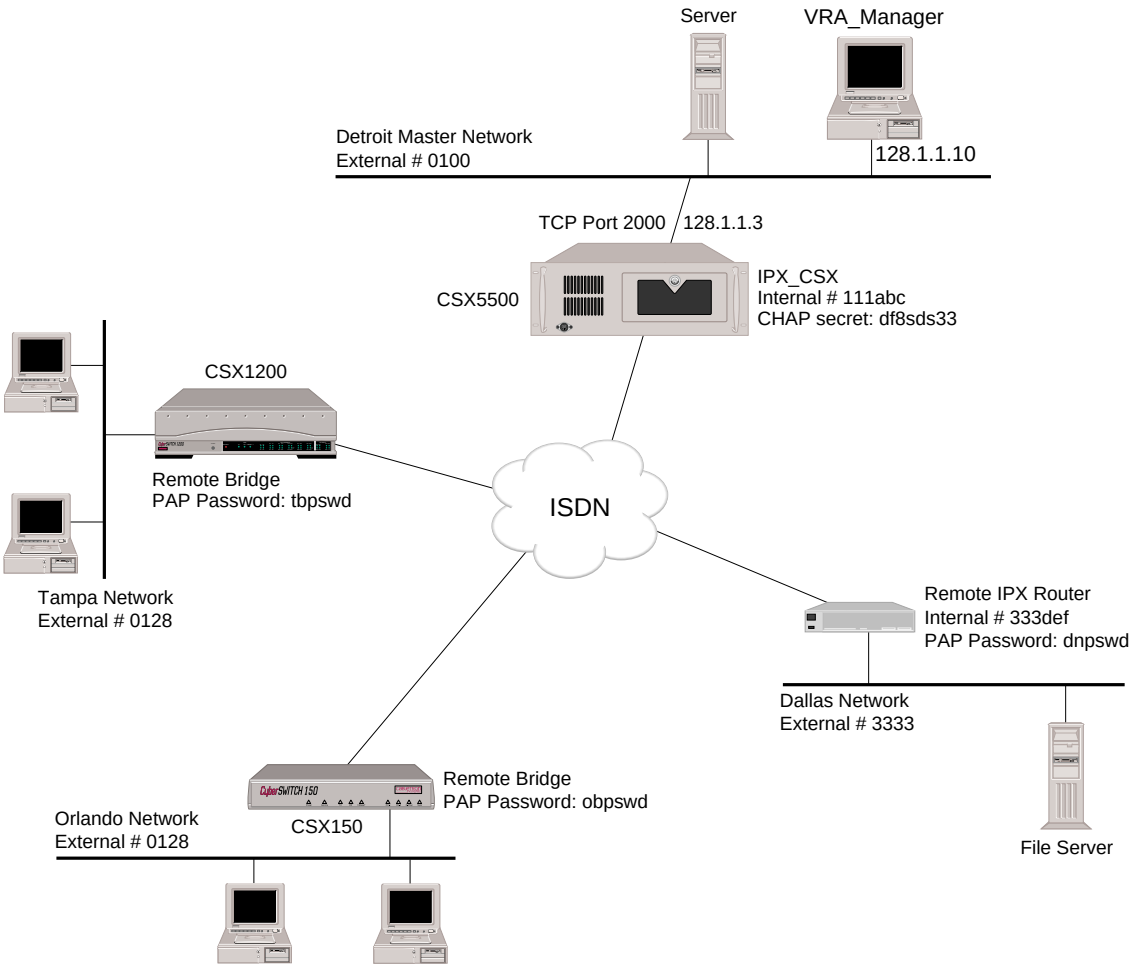
In order for this internetwork to function properly, you must enable bridging and enable IPX on the master network, as well as configure a combination of interfaces and associated users. System details appear in the worksheets, followed by a description of this sample's unique configuration.

INITIAL INSTALLATION STEPS

The first step to configuring a network administered by SFVRA Connection Manager is to fill out the network worksheets located in the CyberSWITCH documentation. Once you complete the worksheets, you may begin installing . The initial steps are basically the same no matter how complicated the network. Refer to the *System Installation* chapter, which describes in detail each of these steps.

A Network Topology worksheet for this network is included on the following page.

NETWORK TOPOLOGY



SYSTEM DETAILS

CyberSWITCH Name	IPX_CSX
LAN IP Address	128.1.1.3
TCP Port Number	2000
CSX - User Group	IPX

RESOURCES

Type	Slot	Switch Type	Synchronization Type
BRI	*1*	*5ESS*	*N/A*
Ethernet-1	*3*	*N/A*	*N/A*

LINES

BRI Lines

Name	Slot	Port	Line type	Call screen	TEI	SPID	Directory number
line1	*1*	*1*	*PPP*		*Auto*		
line2	*1*	*2*	*PPP*		*Auto*		

IPX ROUTING

IPX Routing Information

IPX routing	***X*** enabled ❒ disabled
Internal network number	111abc

Network Interface Information

LAN name	External network number	Remote LAN name	External network number
detroitlan	0100	remotelan	0128

CONFIGURE THE CYBERSWITCH

Configure the CyberSWITCH systems according to the procedures in the appropriate documentation. The purpose of this section is not to describe the configuration steps of CyberSWITCH systems, but to point out the areas that are necessary for the users to gain access under control of the SFVRA-CONN.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH SFVRA-CONN

Using CFGEDIT the following information must be configured for an IPX network to be successful:

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add ETHERNET-1 resource, slot 3

Select Options from the Main Menu
- Select IP Routing
  - Enable IP routing. Define the Interface type to be LAN. Enter *128.1.1.3* as the IP Address. Accept the default RIP Receive Control.

Select Security from the Main Menu
- Select Security Level
  - Enable Device Level Security
- Select System Options and Information
  - Enter *IPX_CSX* as the System Name
- Select Device Level Databases
  - Select VRA Manager as the Authentication Database location.
- Select Off-node Server Information
  - Select VRA Manager and configure *2000* for the TCP Port number.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH IPX USERS

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add a BRI resource, include slot and port numbers and switch type
- Select Current Data Lines
  - Add a line, include the name, slot and port numbers, type, and datalinks, if necessary.

Select Options from the Main Menu
- Select Bridging
  - Enable Bridging
- Select IPX
  - Enable IPX Routing for support across the WAN to the Dallas network. Define the Internal Network Number. Define a LAN interface type, including the name, and external network number, for the LAN IPX Network 0100. Define a WAN (Remote LAN) interface, for support to the Tampa Site.

Note: Security options should not be configured on the CyberSWITCH systems, since SFVRA Connection Manager handles these features.

CONFIGURE THE CYBERSWITCH - USER GROUPING

Note: The SFVRA Connection Manager software should have already been installed, and the Client interface should be activated before proceeding the following steps.

We will begin the network configuration by defining a CyberSWITCH - User Group. These groups can be used to determine which Remote Access Switches users are allowed to call. In this example, we will configure a group based on the user's protocol.

Note: CyberSWITCH - User Groupings can be used for all types of users, from all areas of your network. In this example, we are grouping users by protocol, for ease of understanding the feature only.

1. On the *Tables* menu, select *CyberSWITCH - User Grouping*. The *Table Maintenance* dialog appears.

2. Click *Add*.

3. Enter the name ***IPX***, and click *OK*.

4. Click *Close*.

CONFIGURE THE CYBERSWITCH ON SFVRA-CONN

Note: The Client interface should be activated before proceeding the following steps.

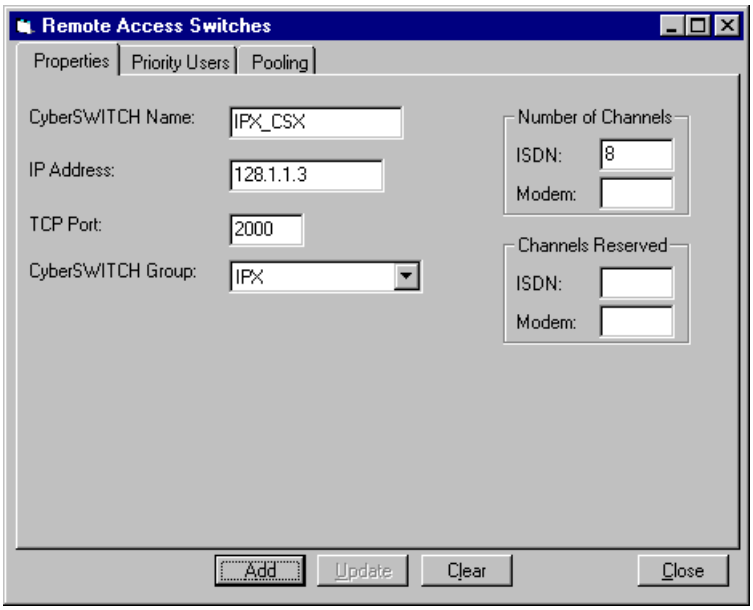
In our example, we only need to supply general properties of the CyberSWITCH in order for SFVRA-CONN to be able to communicate with it. SFVRA-CONN requires a unique name for each CyberSWITCH. It also requires the IP address of the LAN port through which a TCP connection is established to send and receive information. We will also assign the CyberSWITCH to the group that we previously defined. Lastly, in order for the SFVRA-CONN to allow the CyberSWITCH to take incoming calls from users, we must define the number of channels it has available. The Network Topology diagram states that this CyberSWITCH has a BRI resource, which indicates four BRI lines or eight channels available for users. Refer to *Configuring Remote Access Switches* for more information.

1. On the *Functions* menu, select *CyberSWITCH*, or click on the toolbar. The *CyberSWITCH List* dialog appears.

2. Click *Add*. The *Remote Access Switches* dialog appears.

3. Configure CyberSWITCH Properties.

   On the *Properties* tab, enter ***IPX_CSX*** for the *CyberSWITCH Name*. Enter ***128.1.1.3*** for the *IP Address*. Enter ***2000*** for the *TCP Port*. Select ***IPX*** as the *CyberSWITCH Group*. Enter ***8*** for the *Number of ISDN Channels*. The *Properties* tab will appear as follows:



4. Click *Add* and then *Close*.

5. Click *Close* on the *CyberSWITCH List* dialog.

CONFIGURE USER RECORDS

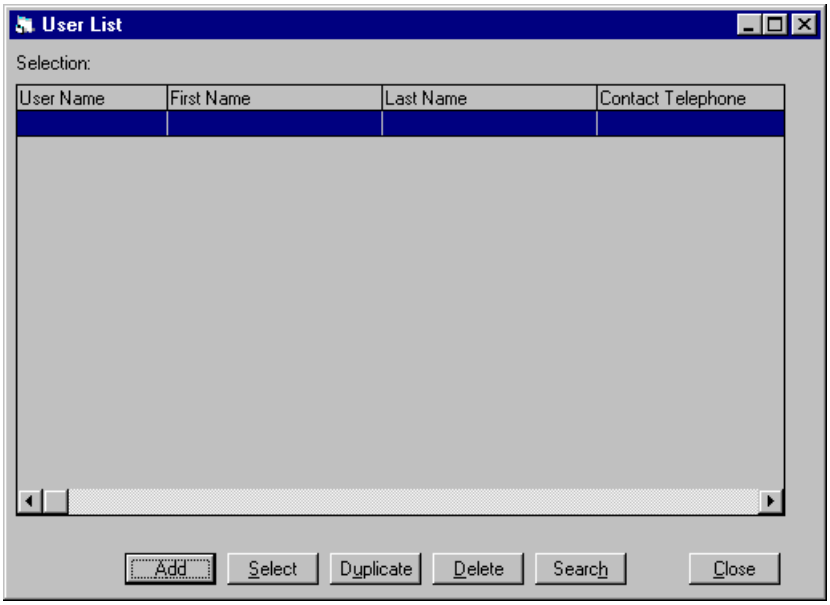
Note: The Client interface should be activated before proceeding the following steps.

In this example, there are two types of IPX users, IPX WAN and Remote LAN. Using the detailed instructions for these steps found in *Configuring Users*, complete the configuration information indicated in the following procedures.

CONFIGURING IPX WAN USERS

The IPX WAN user "dallasnet" is an IPX router with a Novell file server connected to its remote LAN. This user will be configured without call restrictions. A telephone line will be configured so that the central site may call "dallasnet" and use the resources on the remote file server.

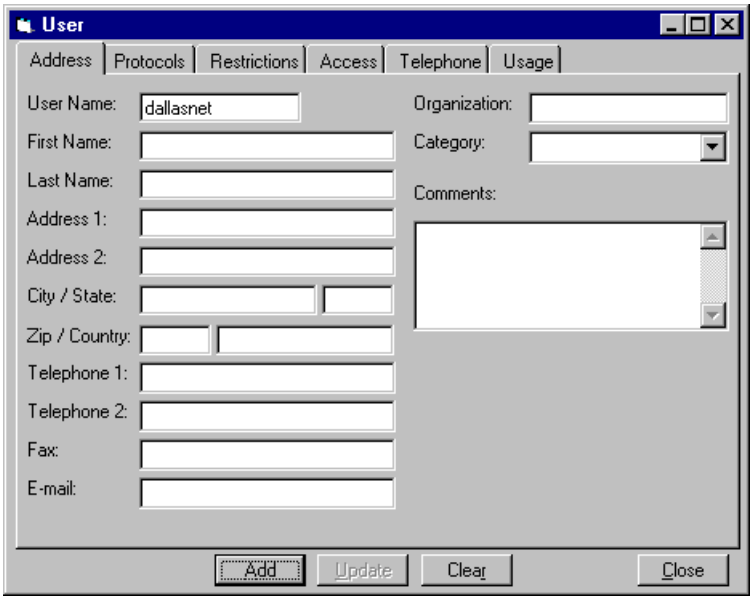
1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog is then displayed as follows:



2. To add remote users, click *Add*. The *User* dialog appears.

3. Define the User Name.

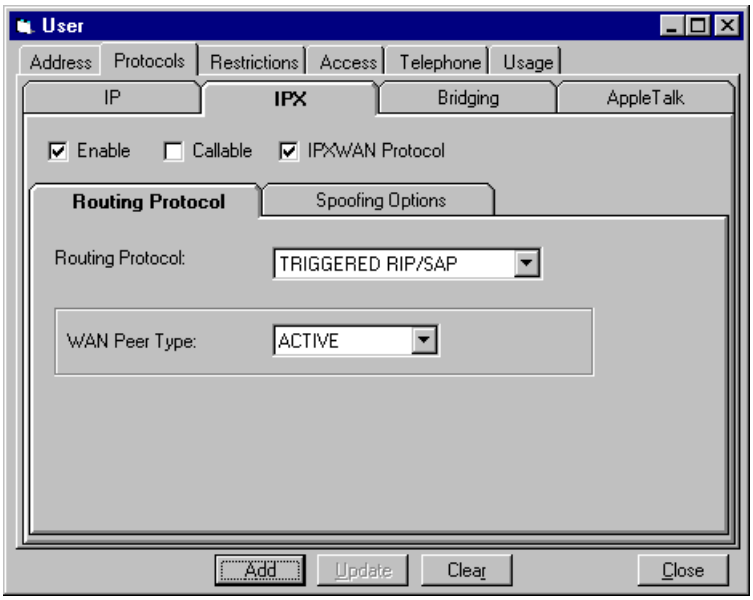
   For this example, we will configure the user "dallasnet" first. On the *Address* tab, enter `dallasnet` for the *User Name*. Only the User Name is required and it must be unique. Other fields are informational for use by the Network Administrator or Help Desk. The *Address* tab should appear as shown below:



4. Enable the IPX Protocol.

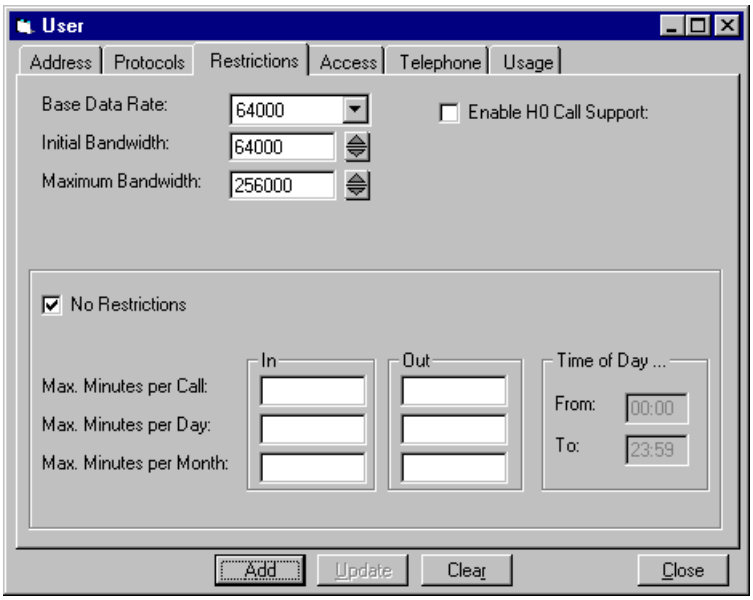
   In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Select *IPX* on the *Protocols* tab and *Enable* IPX and the *IPX WAN Protocol*. Select `Triggered RIP/SAP` as the *Routing Protocol*. Select `ACTIVE` as the *WAN Peer Type*.

   Note: Although "dallasnet" is a callable user, the Callable feature can not be enabled until a telephone number is configured. We will refer back to the IPX tab later on in this example to enable this feature.



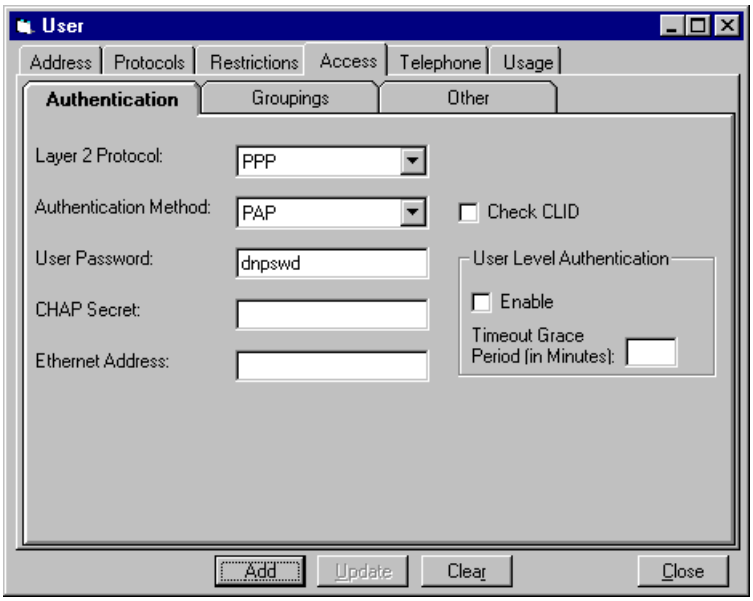
5. Increase the Maximum Bandwidth.

   In this example, user "dallasnet" has no call restrictions and a maximum bandwidth of 256000 bps. Select the *Restrictions* tab and enter the information as it appears below.



6. Configure Authentication for user "dallasnet."

   Select *Authentication* on the *Access* tab. Select *PPP* as the *Layer 2 Protocol*. Select *PAP* as the *Authentication Method*. Enter *dnpswd* for the *User Password.* After the user authentication has been entered, the *Authentication* tab will appear as follows:

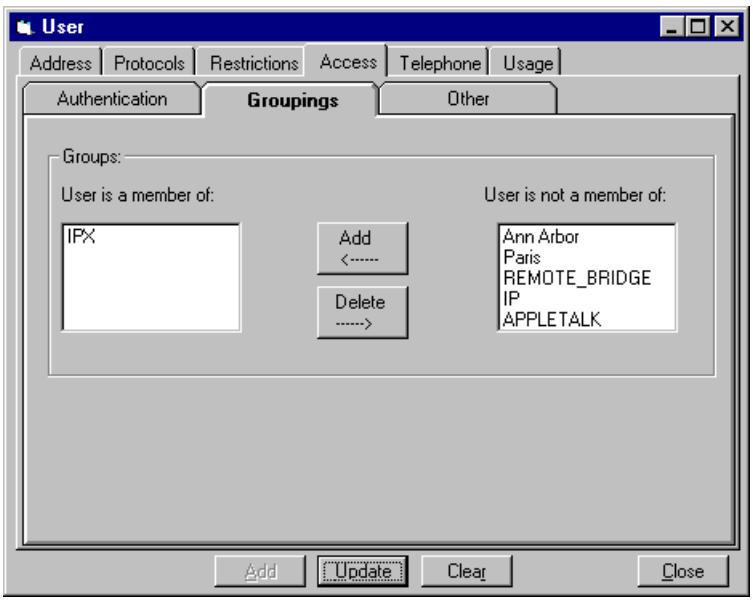


7. Click *Add*.

   Certain user features require the user to be configured in the database before the feature itself can be configured. These feature include: configuring static routes, assigning a user to a group, and configuring telephone numbers and Calling Line ID's. The next parameter that we will configure for user "dallasnet" is the CyberSWITCH - User Group, therefore we need to add the user to the database first.

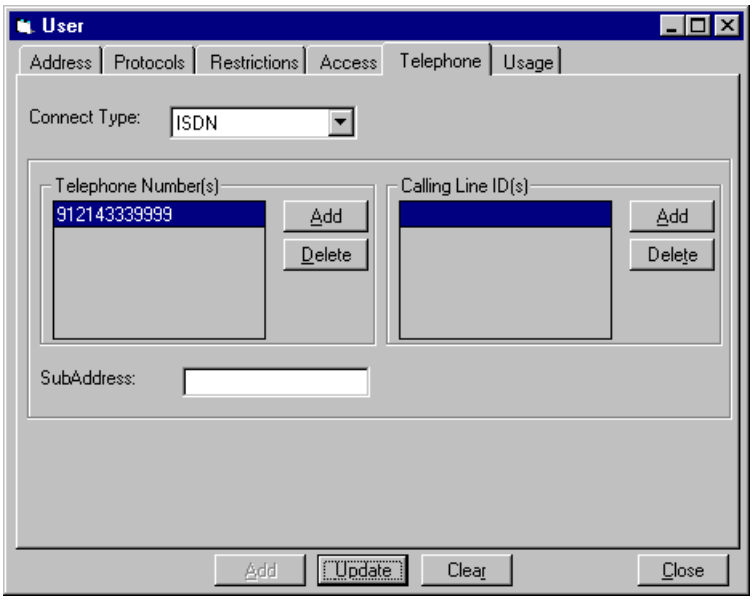
8. Assign the user to a group.

   In order for the user "dallasnet" to be allowed to connect with the CyberSWITCH "IPX_CSX," the user must be in the same group. Select *Groupings* on the *Access* tab. Select *IPX* in the *User is not a member of* box and click *Add*. The *Groupings* tab should appear as shown below:



9. Configure a telephone line for central site calls.

   In order for a CyberSWITCH to call user “dallasnet,” the type of connection needs to be defined and a telephone number for the user must be available. Select the *Telephone* tab. Select *ISDN* as the *Connect Type*. Under *Telephone Number(s)*, click *Add*, enter *912143339999*, and click *OK*.



10. Configure the user “dallasnet” to be callable by the central site.

    Return to *IPX* on the *Protocols* tab. Enable the *Callable* feature.

11. Click *Update* and then click *Close.*

12. Click *Close* on the *User List* dialog.

CONFIGURING REMOTE LAN USERS

The IPX Remote LAN users “tampabr” and "orlandobr" are remote bridges, and will assume the IPX Network Number of the Remote LAN interface on the central site. This user will be configured without call restrictions.

Note: This example only provides screen shots that are distinctly different from those in the previous configuration section. If necessary, refer to the example screens in *Configuring IPX WAN Users* for more detail.

1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog appears.

2. To add remote users, click *Add*. The *User* dialog appears.

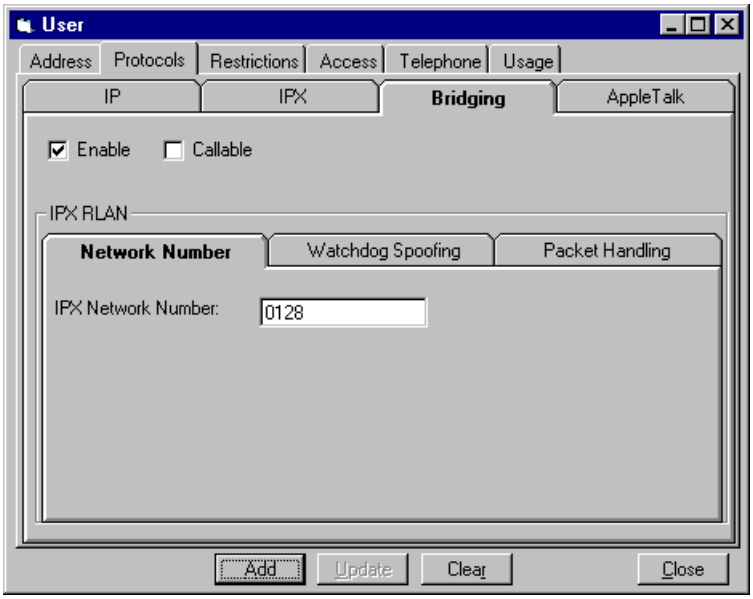
3. Define the User Name.

   On the *Address* tab, enter `tampabr` as the *User Name*. Only the User Name is required and it must be unique. Other fields are informational for use by the Network Administrator or Help Desk.

4. Enable the Bridging Protocol.

   In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Select *Bridging* on the *Protocols* tab and *Enable* the Bridging Protocol. Enter `0128` for the *IPX Network Number*.

Note: An IPX Network Number is not required by this topology, since there isn't a remote file server on this user's LAN. If no Network Number is configured, it will be assigned by the Remote LAN interface connected to the bridge.



5. On the *Restrictions* tab, accept the default values.

6. Configure Authentication for user "tampabr."

   Select *Authentication* on the *Access* tab. Select `PPP` as the *Layer 2 Protocol*. Select `PAP` as the *Authentication Method*. Enter `tbpswd` for the *User Password*.

7. Click *Add*.

   Certain user features require the user to be configured in the database before the feature itself can be configured. These feature include: configuring static routes, assigning a user to a group, and configuring telephone numbers and Calling Line ID's. The next parameter that we will configure for user "tampabr" is the CyberSWITCH - User Group, therefore we need to add the user to the database first.

8. Assign the user to a group.

   In order for the user "tampabr" to be allowed to connect with the CyberSWITCH "IPX_CSX," the user must be in the same group. Select *Groupings* on the *Access* tab. Select `IPX` in the *User is not a member of* box and click *Add*.

9. Click *Update* and then click *Close*.

10. Click *Close* on the *User List* dialog.

Next enter the user information for orlandobr. This user will not have an External Network Number configured. It will assume the Network Number of the RLAN interface that it connects. This user is also a PPP bridge, and is configured using the same authentication as user tampabr, and the password will be obpswd. User orlandobr should be added to the IPX group.

CONFIGURE NETWORK PROXIES

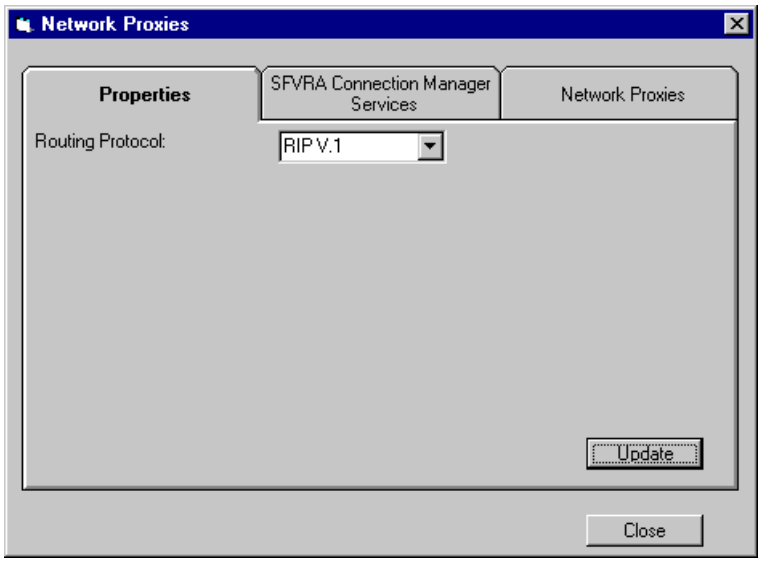
Note: The Client interface should be activated before proceeding the following steps.

Using the detailed instructions for these steps found in *Configuring Network Proxies*, complete the configuration information indicated in the following procedures.

1. On the *Functions* menu, select *Network Proxies*, or click on the toolbar. The *Network Proxies* dialog appears.

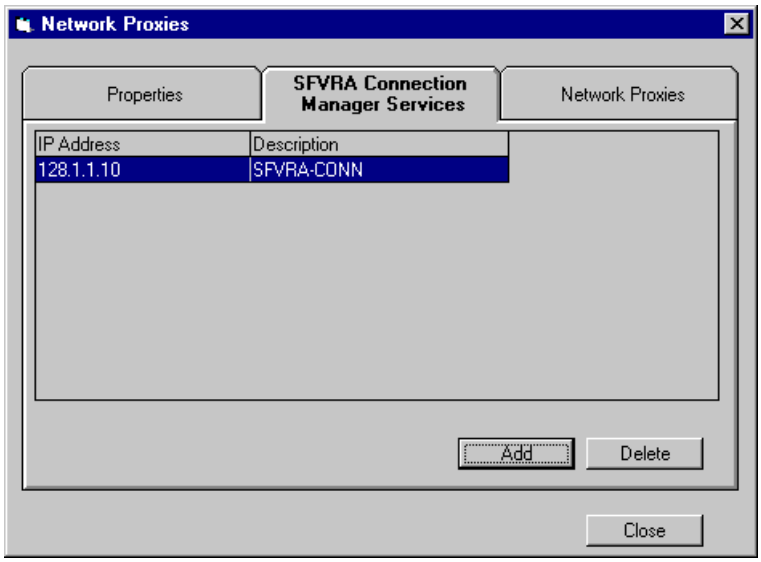
2. Configure basic routing properties.

   On the *Properties* tab, select `RIP V.1` as the *Routing Protocol*.



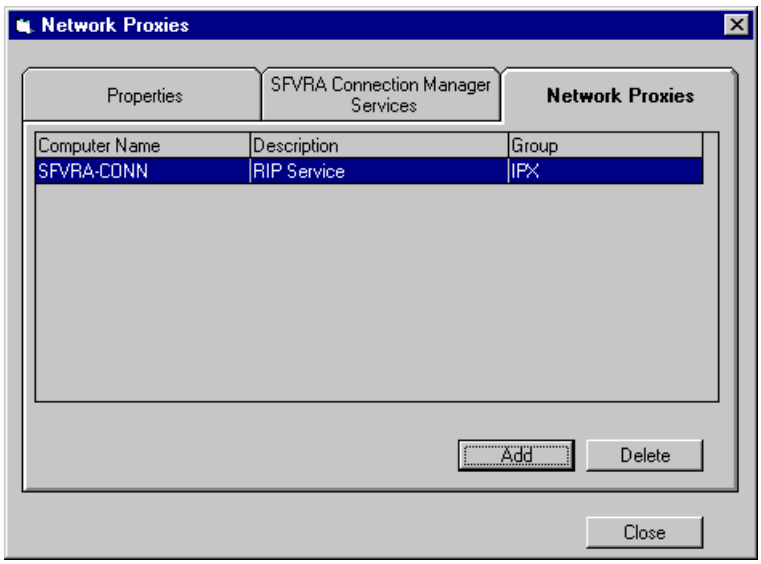
3. Define the location of the SFVRA Service(s).

   Select the *SFVRA Services* tab. Click *Add*. Enter `128.1.1.10` as the *IP Address*. Enter `SFVRA-CONN` for the *Description*. Click *OK*.



4. Assign the RIP Service to a group.

   Select the *RIP Services* tab. Click *Add*. Enter `SFVRA-CONN` for the *Computer Name*. Enter `RIP Service` for the *Description*. Select `IPX` as the *Group*. Click *OK*.



5. Click *Close*.

VERIFY CONFIGURATIONS

Steps on how to verify the installation are detailed in the *System Verification* chapter. Refer to the *System Verification* chapters of your CyberSWITCH documentation for more specific details on verifying the CyberSWITCH features. This section gives an outline of which steps should be executed.

On the SFVRA-CONN Client:

- Check Group assignments

On each system:

- Verify resources are operational
- Verify WAN Lines Available

On IPX_CSX router:

- Check connectivity to local devices
- Check connectivity to Remote LAN sites
- Check connectivity to remote devices
- Check connectivity to *dallasnet* (remote IPX router)

APPLETALK NETWORK EXAMPLE

OVERVIEW

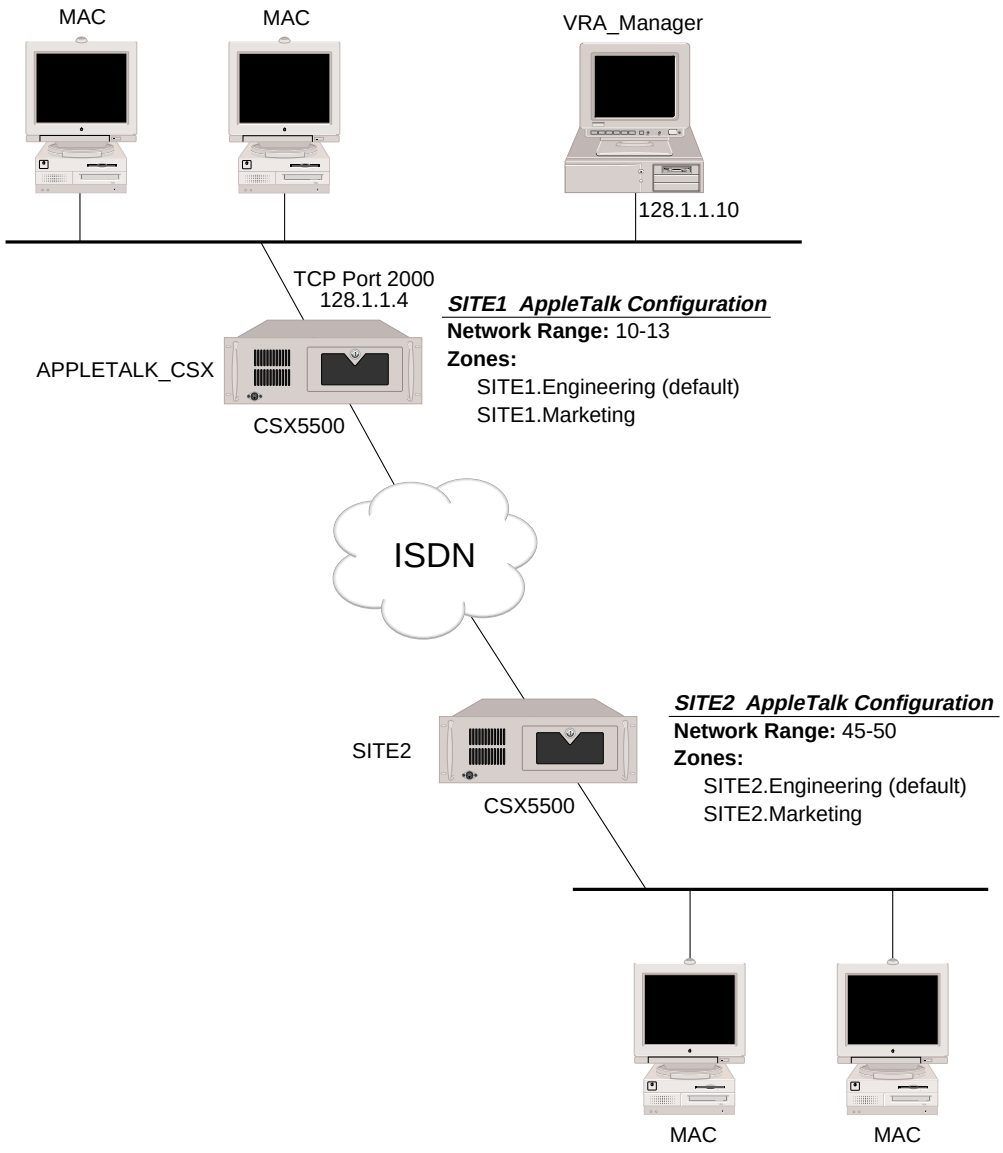
This chapter provides an example configuration of an AppleTalk Routing network. Our AppleTalk network is made up of two LANs, separated by the WAN. The Macs on each side of the WAN need to exchange packets with the MACs on the other side of the WAN. Both LANs also have a CyberSWITCH (SITE1 and SITE2). When configured for AppleTalk routing, SITE1 and SITE2 will provide the access the MACs need.

INITIAL INSTALLATION STEPS

The first step to configuring a network administered by SFVRA Connection Manager is to fill out the network worksheets located in the CyberSWITCH documentation. Once you complete the worksheets, you may begin installing SFVRA-CONN. The initial steps are basically the same no matter how complicated the network. Refer to the *System Installation* chapter, which describes in detail each of these steps.

A Network Topology worksheet for this network is included on the following page.

NETWORK TOPOLOGY



SYSTEM DETAILS

CyberSWITCH Name: APPLETALK_CSX
LAN IP Address: 128.1.1.4
TCP Port Number: 2000
CSX - User Group: APPLETALK

RESOURCES

Type	Slot	Switch Type	Synchronization Type
BRI	*1*	*NI-1*	*N/A*
Ethernet-1	*3*	*N/A*	*N/A*

LINES

BRI Lines

Name	Slot	Port	Line Type	Call Screen	TEI	SPID	Directory Number
Line1	*1*	*1*	*PPP*		*Auto*	*3135551111*	*13135551111**
						3135551112	*13135551112**
Line 2	*1*	*3*	*PPP*		*Auto*	*3135551113*	*13135551113**
						3135551114	*13135551114**
				** Hunt Group Number 13135551111*			

APPLETALK ROUTING

AppleTalk Routing/Port Information

AppleTalk routing	***X*** enabled	❒ disabled		
LAN	Name	*lanport1*		
	Port number	*1*		
	Network type	***X*** extended ❒ nonextended		
	Netwk range/ number	*10-13*		
	AppleTalk address	*(none)*		
	Zone name(s)	*site1.eng*	*site1.mark*	
WAN	Name			
	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			
Unnumbered WAN	***X*** need ❒ don't need			
MAC Dial In WAN	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			

AppleTalk Port Static Routes

Network type to be accessed	Destination network range	Next hop address	Next hop name	Number hops	Zone name(s)
X extended ❒ nonextended	*45-50*	*0.0*	*Site2*	*1*	*site2.eng*
❒ extended ❒ nonextended					
❒ extended ❒ nonextended					

CONFIGURE THE CYBERSWITCH

Configure the CyberSWITCH systems according to the procedures in the appropriate documentation. The purpose of this section is not to describe the configuration steps of CyberSWITCH systems, but to point out the areas that are necessary for the users to gain access under control of the SFVRA-CONN.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH SFVRA-CONN

Using CFGEDIT the following information must be configured for an AppleTalk network to be successful:

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add ETHERNET-1 resource, slot 3

Select Options from the Main Menu
- Select IP
  - Enable IP routing. Define the Interface type to be LAN. Enter *128.1.1.4* as the IP Address. Accept the default RIP Receive Control.

Select Security from the Main Menu
- Select Security Level
  - Enable Device Level Security
- Select System Options and Information
  - Enter *APPLETALK_CSX* as the System Name
- Select Device Level Databases
  - Select VRA Manager as the Authentication Database location.
- Select Off-node Server Information
  - Select VRA Manager and configure *2000* for the TCP Port number.

CONFIGURING THE CYBERSWITCH TO INTERACT WITH APPLETALK USERS

Select Physical Resources from the Main Menu
- Select Current Resources
  - Add a BRI resource, include slot and port numbers and switch type
- Select Current Data Lines
  - Add a line, include the name, slot and port numbers, type, and datalinks, if necessary.

Select Options from the Main Menu
- Select AppleTalk Routing
  - Enable AppleTalk Routing. Define a WAN UnNumbered AppleTalk port.

Note: Security options should not be configured on the CyberSWITCH systems, since SFVRA Connection Manager handles these features.

CONFIGURE THE CYBERSWITCH - USER GROUPING

Note: The SFVRA Connection Manager software should have already been installed, and the Client interface should be activated before proceeding the following steps.

We will begin the network configuration by defining a CyberSWITCH - User Group. These groups can be used to determine which Remote Access Switches users are allowed to call. In this example, we will configure a group based on the user's protocol.

Note: CyberSWITCH - User Groupings can be used for all types of users, from all areas of your network. In this example, we are grouping users by protocol, for ease of understanding the feature only.

1. On the *Tables* menu, select *CyberSWITCH - User Grouping*. The *Table Maintenance* dialog appears.
2. Click *Add*.
3. Enter the name *APPLETALK*, and click *OK*.
4. Click *Close*.

CONFIGURE THE CYBERSWITCH ON SFVRA-CONN

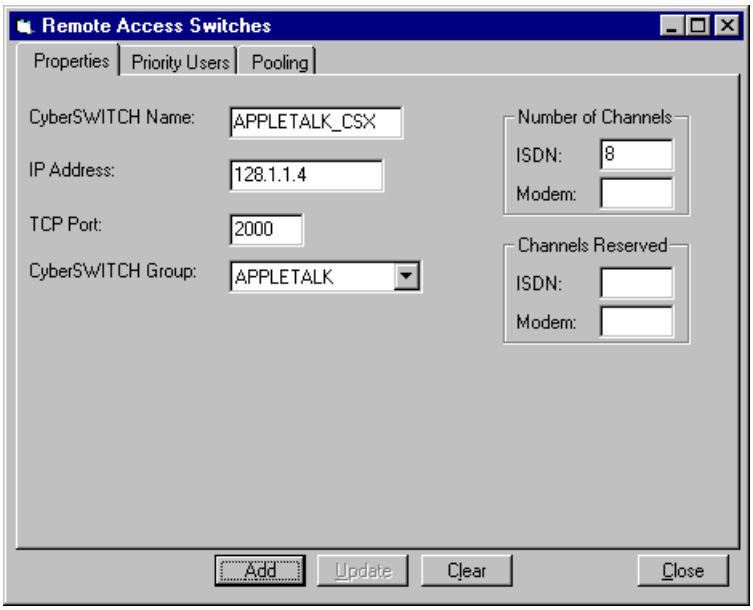
Note: The Client interface should be activated before proceeding the following steps.

In our example, we only need to supply general properties of the CyberSWITCH in order for SFVRA-CONN to be able to communicate with it. SFVRA-CONN requires a unique name for each CyberSWITCH. It also requires the IP address of the LAN port through which a TCP connection is established to send and receive information. We will also assign the CyberSWITCH to the group that we previously defined. Lastly, in order for the SFVRA-CONN to allow the CyberSWITCH to take incoming calls from users, we must define the number of channels it has available. The Network Topology diagram states that this CyberSWITCH has a BRI resource, which indicates four BRI lines or eight channels available for users. Refer to *Configuring Remote Access Switches* for more information.

1. On the *Functions* menu, select *CyberSWITCH*, or click on the toolbar. The *CyberSWITCH List* dialog appears.
2. Click *Add*. The *Remote Access Switches* dialog appears.

3. Configure CyberSWITCH Properties.

   On the *Properties* tab, enter `APPLETALK_CSX` for the *CyberSWITCH Name*. Enter `128.1.1.4` for the *IP Address*. Enter `2000` for the *TCP Port*. Select `APPLETALK` as the *CyberSWITCH Group*. Enter `2` for the *Number of ISDN Channels*. The *Properties* tab will appear as follows:



4. Click *Add* and then *Close*.

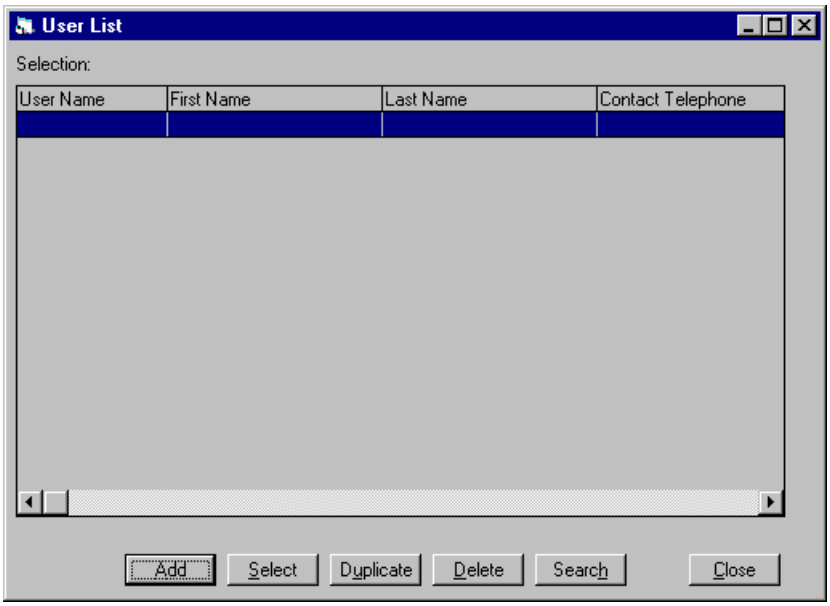
5. Click *Close* on the *CyberSWITCH List* dialog

CONFIGURE USER RECORDS

Note: The Client interface should be activated before proceeding the following steps.

Using the detailed instructions for these steps found in *Configuring Users*, complete the configuration information indicated in the following procedures.

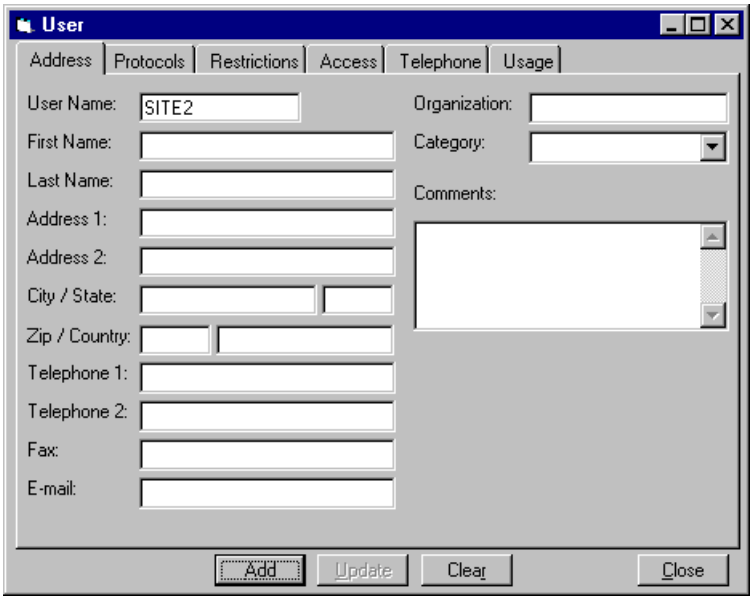
1. On the *Functions* menu, select *Users*, or click on the toolbar. The *User List* dialog is then displayed as follows:



2. To add remote users, click *Add*. The *User* dialog appears.

3. Define the User Name.

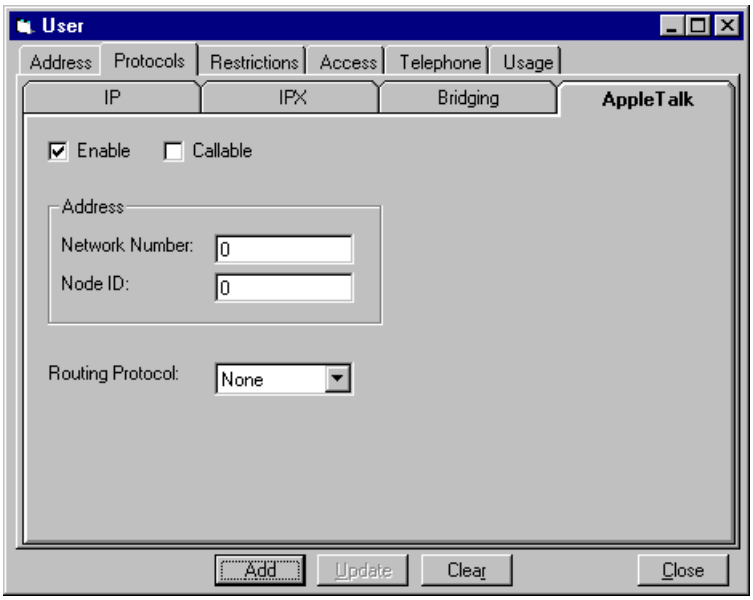
   On the *Address* tab, enter ***SITE2*** for the *User Name*. Only the User Name is required and it must be unique. Other fields are informational for use by the Network Administrator or Help Desk. The *Address* tab should appear as shown below:



4. Enable the AppleTalk Protocol.

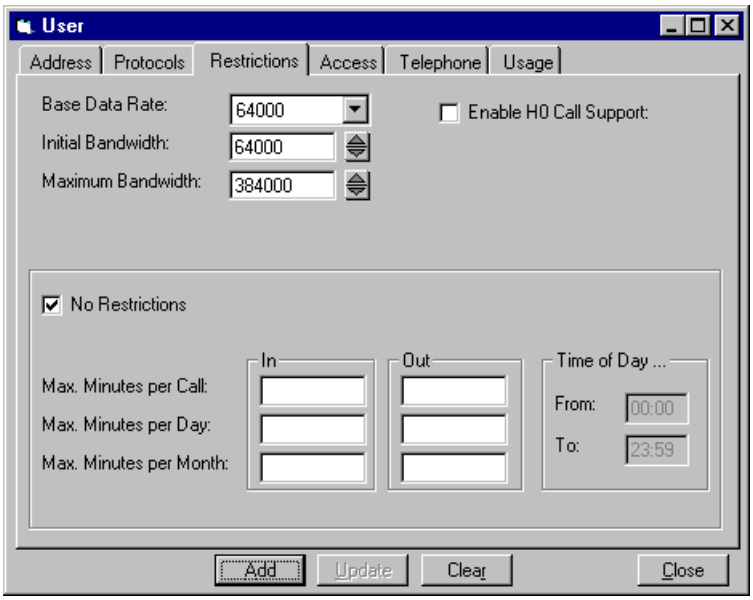
   In order for the Remote Access Switches to be able to communicate with each user, the protocol used by the user needs to be identified. Select *AppleTalk* on the *Protocols* tab and *Enable* AppleTalk. Enter `0` for the *Network Number*. Enter `0` for the *Node ID*. Select `None` as the *Routing Protocol*.

   Note: Although "SITE2" is a callable user, the Callable feature can not be enabled until a telephone number is configured. We will refer back to the AppleTalk tab later on in this example to enable this feature.



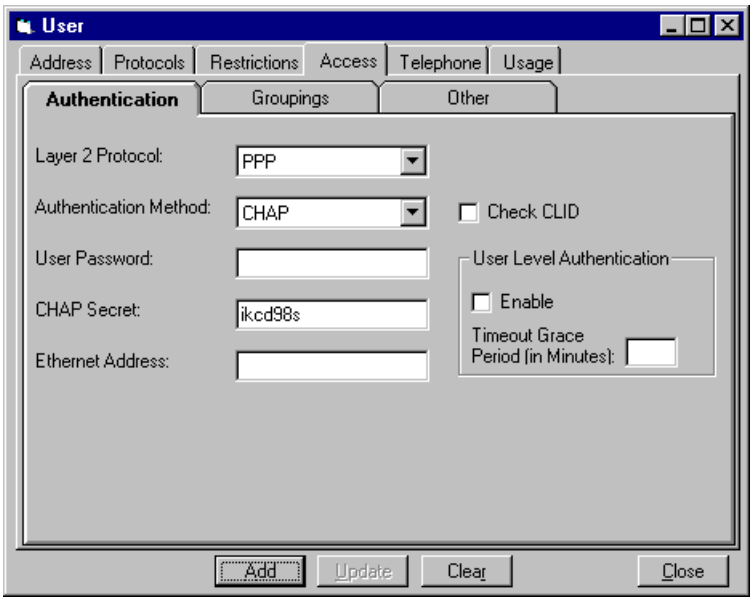
5. Increase the Maximum Bandwidth.

   In this example, user "SITE2" has no call restrictions and a maximum bandwidth of 384000 bps. Select the *Restrictions* tab and enter the information as it appears below.



6. Configure Authentication for user "dallasnet."

   Select *Authentication* on the *Access* tab. Select ***PPP*** as the *Layer 2 Protocol*. Select ***CHAP*** as the *Authentication Method*. Enter ***ikcd98s*** for the *CHAP Secret*. After the user authentication has been entered, the *Authentication* tab will appear as follows:

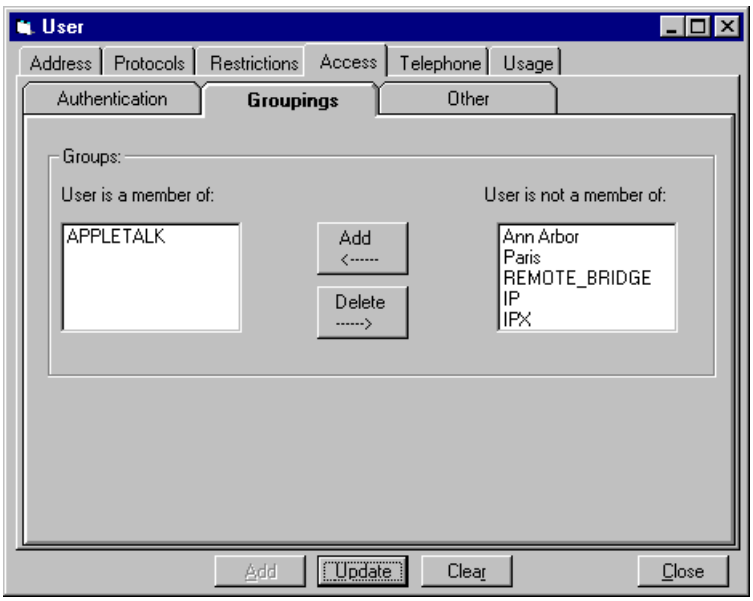


7. Click *Add*.

   Certain user features require the user to be configured in the database before the feature itself can be configured. These feature include: configuring static routes, assigning a user to a group, and configuring telephone numbers and Calling Line ID's. The next parameter that we will configure for user "SITE2" is the CyberSWITCH - User Group, therefore we need to add the user to the database first.

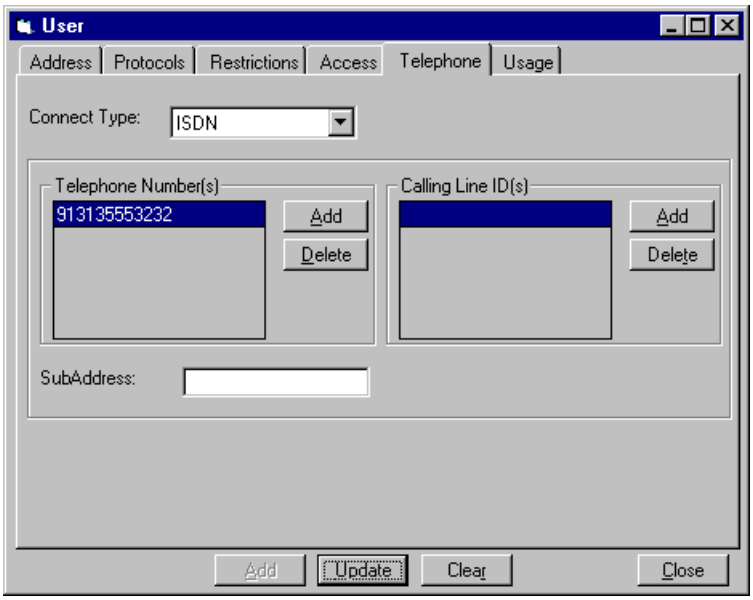
8. Assign the user to a group.

   In order for the user "SITE2" to be allowed to connect with the CyberSWITCH "APPLETALK_CSX," the user must be in the same group. Select *Groupings* on the *Access* tab. Select *APPLETALK* in the *User is not a member of* box and click *Add.* The *Groupings* tab should appear as shown below:



9. Configure a telephone line for central site calls.

   In order for a CyberSWITCH to call user "SITE2," the type of connection needs to be defined and a telephone number for the user must be available. Select the *Telephone* tab. Select *ISDN* as the *Connect Type*. Under *Telephone Number(s)*, click *Add*, enter ***913135553232***, and click *OK*.



10. Configure the user "SITE2" to be callable by the central site.

    Return to *AppleTalk* on the *Protocols* tab. Enable the *Callable* feature.

11. Click *Update* and then click *Close.*

12. Click *Close* on the *User List* dialog.

CONFIGURE NETWORK PROXIES

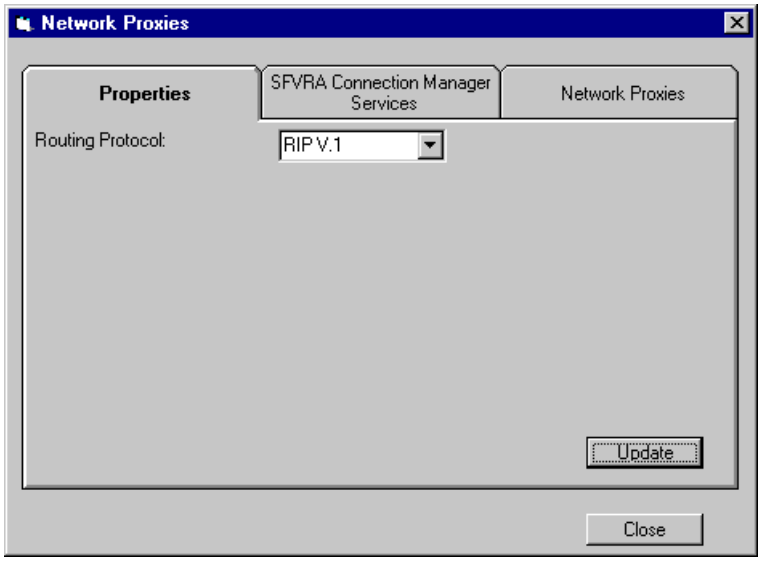
Note: The Client interface should be activated before proceeding the following steps.

Using the detailed instructions for these steps found in *Configuring Network Proxies*, complete the configuration information indicated in the following procedures.

1. On the *Functions* menu, select *Network Proxies*, or click on the toolbar. The *Network Proxies* dialog appears.

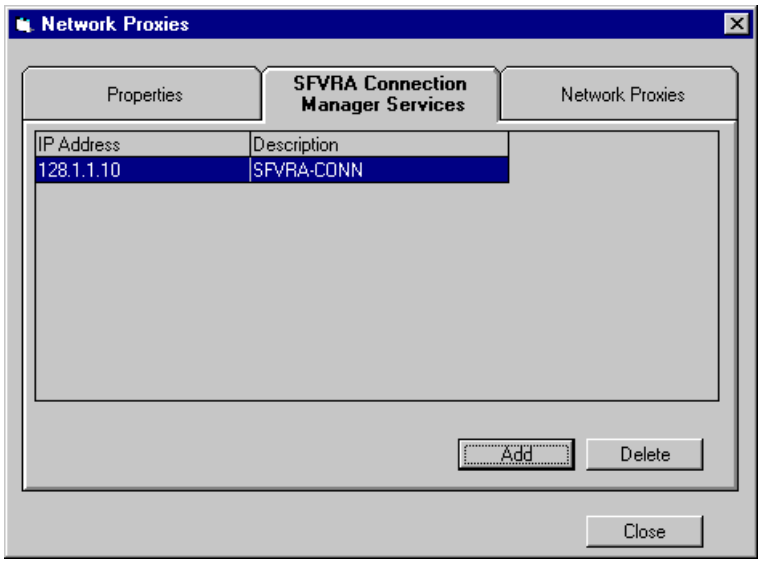
2. Configure basic routing properties.

   On the *Properties* tab, select `RIP V.1` as the *Routing Protocol.*



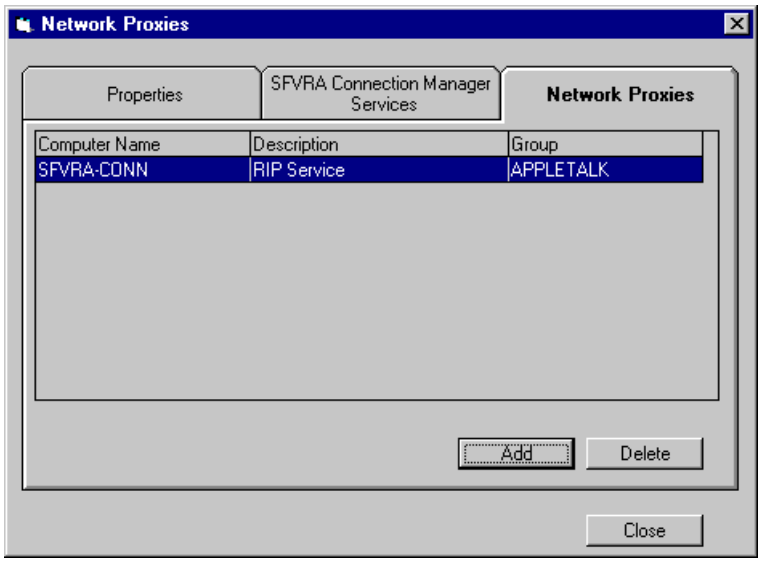
3. Define the location of the SFVRA Service(s).

   Select the *SFVRA Services* tab. Click *Add*. Enter `128.1.1.10` as the *IP Address*. Enter `SFVRA-CONN` for the *Description*. Click *OK*.



4. Assign the RIP Service to a group.

   Select the *Network Proxies* tab. Click *Add*. Enter ***SFVRA-CONN*** for the *Computer Name*. Enter ***RIP Service*** for the *Description*. Select ***APPLETALK*** as the *Group*. Click *OK*.



5. Click *Close*.

VERIFY CONFIGURATIONS

Steps on how to verify the installation are detailed in the *System Verification* chapter. Refer to the *System Verification* chapters of your CyberSWITCH documentation for more specific details on verifying the CyberSWITCH features. This section gives an outline of which steps should be executed.

On the SFVRA-CONN Client:

Check Group assignments

On each system:

Verify resources are operational
Verify WAN Lines Available

SQL DATABASE SCRIPT DEFINITIONS

OVERVIEW

This chapter contains the SQL Database script definitions used to install the SFVRA database. With this information, an advanced SQL administrator may run queries in the ISQL_w application. For example, the administrator may find it convenient to change one field in the database for all users or CyberSWITCH systems with one command, instead of opening each entry in the Client interface. Refer to the SQL Server Administrator's Companion for information on how to run queries.

Note: This chapter contains information about the SFVRA Database Version **4.0** only. Ensure that the version of the SFVRA Database is equivalent.

SFVRA DATABASE TABLES

ACCESS_SERVER

Entries are created in this table by the Client interface when a user configures a CyberSWITCH. The SFVRA Service will only connect via TCP/IP to devices defined in this table.

SERVER_NAME
A string used to identify the name of the CyberSWITCH.

SERVER_IP_ADDR
The IP address SFVRA-CONN uses to create a TCP/IP connection to the CyberSWITCH.

SERVER_SECRET
A string used to do CHAP authentication between the CyberSWITCH and the SFVRA Service. SERVER_SECRET is not currently supported.

NAME_LAST
Identifies a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. NAME_LAST is not currently supported.

NAME_FIRST
Identifies a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. NAME_FIRST is not currently supported.

ADDR1
Identifies the address of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. ADDR1 is not currently supported.

ADDR2
Identifies the address of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. ADDR2 is not currently supported.

POST_CODE
Identifies the ZIP code of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. POST_CODE is not currently supported.

CITY
Identifies the city of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. CITY is not currently supported.

STATE
Identifies the state of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. STATE is not currently supported.

COUNTRY
Identifies the country of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. COUNTRY is not currently supported.

TELEPHONE1
Identifies a telephone number of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. TELEPHONE1 is not currently supported.

TELEPHONE2
Identifies a telephone number of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. TELEPHONE2 is not currently supported.

FAX
Identifies the fax number of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. FAX is not currently supported.

EMAIL
Identifies the email address of a responsible person for the CyberSWITCH. The SFVRA Service does not use this information. EMAIL is not currently supported.

DEMAND_SAMPLE
DEMAND_SAMPLE is currently not supported.

NUM_ISDN_CHAN
The number of ISDN channels for calls that the CyberSWITCH has available. SFVRA uses this number to determine if there is available bandwidth on a CyberSWITCH to make an outgoing call.

NUM_MODEM_CHAN
The number of Modem channels for calls that the CyberSWITCH has available. SFVRA uses this number to determine if there is available bandwidth on a CyberSWITCH to make an outgoing call.

ISDN_CHAN_RESERVED
The number of ISDN channels that should be reserved on a CyberSWITCH to be used only by priority users listed in the USER_RESERVED table where SERVER_NAME matches.

MODEM_CHAN_RESERVED
The number of Modem channels that should be reserved on a CyberSWITCH to be used only by priority users listed in the USER_RESERVED table where SERVER_NAME matches.

SERVER_TCP_PORT
The TCP port SFVRA-CONN uses to create the TCP/IP connection to the CyberSWITCH.

IP_POOL_START
The first address used to create a pool of addresses in the IP_POOL table for the CyberSWITCH.

IP_POOL_END
The last address used to create a pool of addresses in the IP_POOL table for the CyberSWITCH.

ENABLE_DYN_IP_ADDR
Indicates if IP Pooling is enabled or disabled for the CyberSWITCH. If enabled, an entry is created in the IP_POOL table for each address between IP_POOL_START and IP_POOL_END for the SERVER_NAME. A value of TRUE indicates that IP Pooling is enabled, while FALSE means it is disabled.

GROUP_ID
Represents the group to which the CyberSWITCH belongs. This correlates to the GROUP_ID field in the GROUPS table.

STATUS
Indicates the current state of the TCP/IP connection between the CyberSWITCH and SFVRA Connection Manager. "0" indicates that the SFVRA Service recognizes the CyberSWITCH in the database, but there is currently no TCP/IP connection between the CyberSWITCH and SFVRA-CONN. "1" indicates that a TCP/IP connection has been established between the CyberSWITCH and SFVRA-CONN. "2" indicates that the CyberSWITCH was recently added to the SFVRA database, but the SFVRA Service has detected it yet.

ACCESS_SERVER_STATUS

The SFVRA Service creates entries in this table when calls are active to a CyberSWITCH.

SERVER_NAME
The CyberSWITCH to which this entry belongs.

ISDN_CHAN_IN_USE
The current number of ISDN channels in use by the CyberSWITCH.

MODEM_CHAN_IN_USE
The current number of Modem channels in use by the CyberSWITCH.

CALLING_NUMBERS

Entries are created in this table by the Client interface when a user is configured to have either telephone numbers or CLIDs.

USER_NAME
The user to which this number belongs.

NUMBER_TYPE
Defines the type of number for the User. Refer to the Number Type options table below to translate the number type codes.

Code	Number Type Options
1	Telephone Number
2	Calling Line ID

CALLNUMBER
The number.

IP_POOL

Entries are created in this table by the Client interface when the IP Address Pool is enabled for a CyberSWITCH.

SERVER_NAME
The CyberSWITCH to which the IP address belongs.

IP_ADDR
The IP address in the pool currently being used by USER_NAME.

USER_NAME
The user that is using the IP address from the pool. If NULL, then the address is not in use and SFVRA-CONN may assign the number to a user when a call is initiated between the CyberSWITCH and a user that has the ASSIGN_IP_ADDR field of the USER_ACCESS table set to true.

STATIC_IP_ROUTES

Entries are created in this table by the Client interface when a user has IP static routes configured.

USER_NAME
The user to which this static route belongs.

DEST_SUBNET
The destination subnet of the static route.

SUBNET_MASK
The subnet mask of the static route.

METRIC
The metric value of the static route.

PROBLEM_LIST

The SFVRA Service creates entries in this table whenever a call has some type of problem.

SERVER_NAME
The CyberSWITCH involved in this problem.

USER_NAME
The user involved in this problem.

CONNECT_ID
The Connect ID on the CyberSWITCH that had the problem. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a connection on a CyberSWITCH and is of no informative purpose to the customer.

CALL_ID
The Call ID on the CyberSWITCH that had the problem. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a call on a CyberSWITCH and is of no informative purpose to the customer.

START_TIME
The start time of the call that had the problem.

CALLING_TN
The calling telephone number that had the problem.

FAILURE_TYPE_ID
A number matching an entry in the FAILURE_TYPES table for the problem.

REASON_STRING
A string gleaned from the REASON_STRINGS table for the problem.

FAILURE_TYPES

Entries are created in this table when the database is installed or upgraded. The SFVRA Service and the Client interface use these entries to log and display errors.

FAILURE_TYPE_ID
A unique number used to identify a failure string.

FAILURE_TYPE
The failure.

REASON_STRINGS

Entries are created in this table when the database is installed or upgraded. The SFVRA Service and the Client interface use these entries to log and display the reasons for the errors.

REASON_CODE
A unique number used to identify a reason for an error.

REASON_STRING
The reason for the failure.

CALL_HISTORY

The SFVRA Service creates entries in this table when a connection has gone down. All calls that made up this connection are moved from the CURRENT_CALL table to this table.

CALLNR
An identity field to uniquely identify this entry.

CONNECTNR
The number that ties the call to the connection in the CONNECT_HISTORY table.

CONNECT_ID
The Connect ID on the CyberSWITCH for the call. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a connection on a CyberSWITCH and is of no informative purpose to the customer.

CALL_ID
The Call ID on the CyberSWITCH for the call. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a call on a CyberSWITCH and is of no informative purpose to the customer.

CALL_START_TIME
The start time of the call.

CALL_END_TIME
The end time of the call.

DURATION
The duration of this call, the difference between CALL_START_TIME and CALL_END_TIME.

BANDWIDTH
The maximum bandwidth used by this call.

CALLED_TN
The number that was called.

CALLING_TN
The number that made the call.

FWD_TN
The number from which the call was forwarded.

CONN_START_TIME
The start time of the connection that this call is a part. This is the same value as START_TIME in the CONNECTION_HISTORY table.

CALL_DIRECTION
A string representing the direction of the call. IN stands for a call made in to a CyberSWITCH from a remote user. OUT means that the CyberSWITCH made a call out to a remote user. DEDICATED indicates a dedicated line.

ADVICE_OF_CHARGES
A number returned from the phone switch about the cost of the call. Note that this is only applicable in Japan.

IN_OCTET_COUNT
The number of octets of data that was received by the CyberSWITCH during the call.

OUT_OCTET_COUNT
The number of octets of data that was transmitted by the CyberSWITCH during the call.

CONNECT_HISTORY

The SFVRA Service creates the entries in this table when a connection goes down. The connection is moved from the CURRENT_CONNECT table to this table.

CONNECTNR
A number from the CURRENT_CONNECT table that uniquely identifies this entry. Used in the CALL_HISTORY table to reference all calls that made up the connection.

USER_NAME
The User that was part of the connection.

SERVER_NAME
The CyberSWITCH that was part of the connection.

CONNECT_ID
The Connection ID on the CyberSWITCH for the connection. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a connection on a CyberSWITCH and is of no informative purpose to the customer.

START_TIME
The start time of the connection.

END_TIME
The end time of the connection.

DURATION
The duration of the connection is the difference between the START_TIME and the END_TIME.

CONNECT_TYPE
A number that references the CONECTTYPE_ID in the USER_CONNECTTYPES table.

CALL_DIRECTION
A string that represents the direction of the call that initiated the connection. IN stands for a call made in to a CyberSWITCH from a remote user. OUT means that the CyberSWITCH made a call out to a remote user. DEDICATED indicates a dedicated line.

MAX_BANDWIDTH
A number that represents the maximum bandwidth that was ever used during the connection.

IN_OCTET_COUNT
The number of octets of data received by the CyberSWITCH during the connection.

OUT_OCTET_COUNT
The number of octets of data transmitted by the CyberSWITCH during the connection.

IP_ADDRESS
The IP address of the remote user involved in the connection. This field is useful for identifying the IP address of remote users that request an IP address from a pool of addresses. The default value for non-IP remote users is 0.0.0.0.

CURRENT_CALL

The SFVRA Service creates these entries when a call comes up. The entries stay in this table until the connection goes down at which time they move to the CALL_HISTORY table.

CONNECTNR
The number that ties the call to the connection in the CURRENT_CONNECT table.

USER_NAME
The User that is part of the call.

SERVER_NAME
The CyberSWITCH that is part of the call.

CONNECT_ID
The Connect ID on the CyberSWITCH for the connection. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a connection on a CyberSWITCH and is of no informative purpose to the customer.

CALL_ID
The Call ID on the CyberSWITCH for the call. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a connection on a CyberSWITCH and is of no informative purpose to the customer.

START_TIME
The start time of the call.

BANDWIDTH
The bandwidth of the call.

CALLED_TN
The number that was called for the call.

CALLING_TN
The number that made the call.

FWD_TN
The number from which the call was forwarded.

CALLDIRECTION_ID
The direction of the call as referenced in the USER_CALLDIRECTIONS table.

CALL_STATUS
The current status of the call. Active means that the call is currently in place. Dropped means that as bandwidth decreases, calls within a connection may be dropped. Unknown means the call is in an unknown state. The unknown state is entered for any call that was Active when the TCP connection between the CyberSWITCH and the SFVRA-CONN was lost.

ADVICE_OF_CHARGES
A number returned from the phone switch about the cost of the call. Note that this is only applicable in Japan.

TX_ID
A number uniquely identifying the call on the CyberSWITCH. The CyberSWITCH sends this number when the call is initiated.

DURATION
The duration of the call is the difference between the START_TIME and the CALL_END_TIME. The duration is only valid if the call is in the DROPPED CALL_STATUS state.

CALL_END_TIME
The end time of the call. The end time of the call is only valid if the call is in the DROPPED CALL_STATUS state.

IN_OCTET_COUNT
The number of octets of data received by the CyberSWITCH during the call. The received octet count is only valid if the call is in the DROPPED CALL_STATUS state.

OUT_OCTET_COUNT
The number of octets of data transmitted by the CyberSWITCH during the call. The transmitted octet count is only valid if the call is in the DROPPED CALL_STATUS state.

CONNECTTYPE_ID
The type of connection as referenced in the USER_CONNECTTYPES table.

CURRENT_CONNECT

The SFVRA Service creates these entries when a connection goes up. The entries remain in this table until the connection goes down at which time they entry moves to the CONNECT_HISTORY table.

CONNECTNR
An Identity field to uniquely identify this entry form other entries. ConnectNr is used in the CURRENT_CALL table to reference all the calls that make up this connection.

USER_NAME
The User that is part of the connection.

SERVER_NAME
The CyberSWITCH that is part of the connection.

CONNECT_ID
The Connect ID on the CyberSWITCH for the connection. This number is an index into an array on the CyberSWITCH. It is used by the SFVRA Service to uniquely identify a connection on a CyberSWITCH and is of no informative purpose to the customer.

START_TIME
The start time of the connection.

CONNECTTYPE_ID
The type of the call that initiated the connection as referenced in the USER_CONNECTTYPES table.

CALLDIRECTION_ID
The direction of the call that initiated the connection as reference in the USER_CALLDIRECTIONS table.

CURRENT_BANDWIDTH
A number that represents the current bandwidth of the connection. This number is updated each time a call goes up or down.

MAX_BANDWIDTH
A number that represents the maximum bandwidth that has been used so far during the connection. This number is updated each time a call goes up or down.

CONNECT_STATUS
The current status of the connection. Active means that the connection is currently in place. Dropped means that as bandwidth decreases, calls within a connection may be dropped. Unknown means the connection is in an unknown state. The unknown state is entered for any connection that was Active when the TCP connection between the CyberSWITCH and the SFVRA-CONN was lost.

IN_OCTET_COUNT
The number of octets of data received by the CyberSWITCH during the connection.

OUT_OCTET_COUNT
The number of octets of data transmitted by the CyberSWITCH during the connection.

IP_ADDRESS
The IP address of the remote user involved in the connection. This field is useful for identifying the IP address of remote users that request an IP address from a pool of addresses. The default value for non-IP remote users is 0.0.0.0.

USER_ACCESS

Entries are created in this table by the Client interface for every User configured.

Note: For every entry in USER_ACCESS there must be a corresponding entry in the USER_INFO table.

USER_NAME
A string used to uniquely identify a User.

AUTHENTICATION_ID
A number that represents the type of authentication to perform when a call is being negotiated to or from the user.

ID	Authentication Type
1	Password Authentication Protocol (PAP)
2	Challenge Handshake Authentication Protocol (CHAP)
3	Calling Line ID (CLID)
4	None
5	Combinet Proprietary Protocol (CPP
6	NT

USER_PASSWORD
A string used for PAP or NT Authentication. This string is only used if the AUTHENTICATION_ID indicates PAP or NT Authentication.

SECRET
A string used for CHAP Authentication. This string is only used if the AUTHENTICATION_ID indicates CHAP Authentication.

MINUTES_IN_CALL
A number that indicates the maximum number of minutes an incoming call will be allowed. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

MINUTES_IN_DAY
A number that indicates the maximum number of minutes incoming calls will be allowed in any given day. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

MINUTES_IN_MONTH
A number that indicates the maximum number of minutes incoming calls will be allowed in any given month. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

MINUTES_OUT_CALL
A number that indicates the maximum number of minutes an outgoing call will be allowed. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

MINUTES_OUT_DAY
A number that indicates the maximum number of minutes outgoing calls will be allowed on any given day. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

MINUTES_OUT_MONTH
A number that indicates the maximum number of minutes outgoing calls will be allowed in any given month. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

IP_ADDRESS
The IP address of the user.

LAYER2_ID
A number that indicates the type of layer 2 protocol to negotiate with this user.

ID	Layer 2 Protocol
0	Point to Point Protocol (PPP)
1	Combinet Proprietary Protocol (CPP)

ETHERNET_ADDR
The Ethernet address of the User. Note that this value is only valid if AUTHENTICATION_ID indicates CPP authentication.

ENABLE_COMPRESSION
Indicates if compression is enabled or disabled for the User. A value of TRUE indicates that compression is enabled, while FALSE means it is disabled. ENABLE_COMPRESSION is not currently supported.

ENABLE_MLP
Indicates if the Multi-Link Protocol (MLP) is enabled or disabled for the User. A value of TRUE indicates that MLP is enabled, while FALSE means it is disabled. ENABLE_MLP is not currently supported.

ENABLE_IP
Indicates if the IP Protocol is enabled or disabled for the User. A value of TRUE indicates that the IP Protocol is enabled, while FALSE means it is disabled.

ENABLE_BRIDGE
Indicates if the Bridging protocol is enabled or disabled for the User. A value of TRUE indicates that the Bridging protocol is enabled, while FALSE means it is disabled.

CALL_IP
Indicates if calls can or can not be initiated to this User based on an IP packet. A value of TRUE indicates that calls can be initiated to the User based on an IP packet, while FALSE means calls can not be initiated.

CALL_BRIDGE
Indicates if calls can or can not be initiated to this User based on a bridge packet. A value of TRUE indicates that calls can be initiated to the User based on a bridge packet, while FALSE means calls can not be initiated.

CALL_OUT
CALL_OUT is not currently supported.

CALL_BACK
CALL_BACK is not currently supported.

INIT_BANDWIDTH
A number that represents the bandwidth to be instigated whenever a CyberSWITCH initiates a call to the User.

MAX_BANDWIDTH
A number that represents the maximum bandwidth that will ever be allowed to the User.

CONNECTYPE_ID
A number that references the CONNECTTYPE_ID in the USER_CONNECTTYPES table that indicates what type of connection to make with the User.

BASE_DATARATE
A number indicating the base data rate of connections for the User.

TOD_NOT_BEFORE
The number of minutes since midnight before which a User is not allowed connections. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

TOD_NOT_AFTER
The number of minutes since midnight after which a User is not allowed connections. Note that this is only valid if NO_RESTRICTIONS is set to FALSE.

NO_RESTRICTIONS
Indicates if call restrictions are enabled or disabled. A value of TRUE indicates that no call restrictions are enabled, while FALSE means they are disabled. If the value is FALSE, the following fields are used: MINUTES_IN_CALL, MINUTES_IN_DAY, MINUTES_IN_MONTH, MINUTES_OUT_CALL, MINUTES_OUT_DAY, MINUTES_OUT_MONTH, TOD_NOT_BEFORE, and TOD_NOT_AFTER

ASSIGN_IP_ADDR
Indicates if the user should be assigned an IP address from the CyberSWITCH or not. A value of TRUE indicates that the User does require that an IP address be assigned, while FALSE means that the User does not need an address.

CHECK_CLID
Indicates if a call with the User will include CLID security. A value of TRUE indicates that a call from this user will require CLID security, while FALSE means it does not.

SUB_ADDRESS
The sub address of the telephone number for the User.

COMPRESSION_SEED
A number that represents the starting PPP STAC-LZS Sequence Number.

ENABLE_IPX
Indicates if the IPX Protocol is enabled or disabled for the User. A value of TRUE indicates that the IPX Protocol is enabled, while FALSE means it is disabled.

CALL_IPX
Indicates if calls can or can not be initiated to this User based on an IPX packet. A value of TRUE indicates that calls can be initiated to the User based on an IPX packet, while FALSE means calls can not be initiated.

SPOOF_WD_DEFAULT_IPX
Indicates how a CyberSWITCH should handle IPX Watchdog Protocol when there is no connection established with the User. Refer to the Spoofing options table below to translate the spoofing codes.

Code	Spoofing Options
1	Forward
2	Spoof
3	Discard

SPOOF_WD_CONNECT_IPX
Indicates how a CyberSWITCH should handle IPX Watchdog Spoofing while there is a connection to the User. Refer to the Spoofing options table above to translate the spoofing codes.

SPOOF_WD_SPECIAL_IPX
Indicates how a CyberSWITCH should handle IPX Watchdog Spoofing during the special period after disconnecting. Refer to the Spoofing options table above to translate the spoofing codes.

SPOOF_WD_SPECIAL_TIME_IPX
A number that indicates the length of the special period in minutes after disconnecting from this User for IPX Watchdog Spoofing.

SPOOF_WD_DEFAULT_SPX
Indicates how a CyberSWITCH should handle SPX Watchdog Protocol when there is no connection established with the User. Refer to the Spoofing options table above to translate the spoofing codes.

SPOOF_WD_CONNECT_SPX
Indicates how a CyberSWITCH should handle SPX Watchdog Spoofing while there is a connection to the User. Refer to the Spoofing options table above to translate the spoofing codes.

SPOOF_WD_SPECIAL_SPX
Indicates how a CyberSWITCH should handle SPX Watchdog Spoofing during the special period after disconnecting. Refer to the Spoofing options table above to translate the spoofing codes.

SPOOF_WD_SPECIAL_TIME_SPX
A number that indicates the length of the special period in minutes after disconnecting from this User for SPX Watchdog Spoofing.

SPOOF_IPX_SERIAL_PACKET
Indicates how a CyberSWITCH should handle Serialization packets, which are used to detect unauthorized duplication of NetWare Software. Refer to the packet handling options table below to translate the packet handling codes.

Code	Packet Handling Options
1	Always Discard
2	Forward Only When Connected
3	Always Forward

SPOOF_IPX_MESSAGE_PACKET
Indicates how a CyberSWITCH should handle Message Waiting packets, which are sent by servers to attached clients to inform them that the server has a message to send to them. Refer to the packet handling options table above to translate the packet handling codes.

DM_BEARER
Describes the bearer capabilities for the User's modem. Refer to the modem bearer capabilities table below to translate the bearer codes. Note that this is only valid when CONNECTTPE_ID is set to 3 (Digital Modem).

Code	Modem Bearer Capabilities
0	Speech
10 hex	3.1 kHz Audio

DM_BAUD_RATE
Defines the baud rate for the User's modem. Currently, the only setting is 0 (Auto). Note that this is only valid when CONNECTTYPE_ID is set to 3 (Digital Modem).

H0_SUPPORT
Indicates if H0 Call Support is enabled or disabled for the User. A value of TRUE indicates that H0 Call Support is enabled, while FALSE means it is disabled.

IP_FILTER_IN
A string that defines an IP Input Filter, which monitors packets that this User sends into SFVRA-CONN's local subnet.

IP_FILTER_OUT
A string that defines an IP Output Filter, which monitors packets that this User receives out from the SFVRA-CONN's local subnet.

IPX_WAN
Indicates if the IPXWAN Protocol is enabled or disabled for the User. A value of TRUE indicates that the IPXWAN Protocol is enabled, while FALSE means it is disabled.

IPX_ROUTING_PROTOCOL
Defines the IPX Routing Protocol for the User. Refer to the IPX Routing Protocol options table below to translate the routing protocol codes.

Code	IPX Routing Protocol Options
1	None
2	RIP / SAP
3	Triggered RIP / SAP

IPX_TRIGGER_TYPE
Defines the WAN Peer type for the User. Refer to the WAN Peer Type options table below to translate the peer type codes.

Code	WAN Peer Type Options
0	Passive
1	Active

IPX_NETWORK_NUMBER
A decimal number that represents the hexadecimal IPX Remote LAN Network Number for the User.

GROUP_ID
A number matching in the GROUPS table to which the User belongs. Zero (0) implies that the User belongs to multiple groups and those entries can be found in the USER_GROUPS table.

ENABLE_ATALK
Indicates if the AppleTalk Protocol is enabled or disabled for the User. A value of TRUE indicates that the AppleTalk Protocol is enabled, while FALSE means it is disabled.

CALL_ATALK
Indicates if calls can or can not be initiated to this User based on an AppleTalk packet. A value of TRUE indicates that calls can be initiated to the User based on an AppleTalk packet, while FALSE means calls can not be initiated.

ATALK_ROUTING_PROTOCOL
Defines the AppleTalk Routing Protocol for the User. Refer to the AppleTalk Routing Protocol options table below to translate the peer type codes.

Code	AppleTalk Routing Protocol Options
0	None
1	RTMP

ATALK_NODE
A number that represents the AppleTalk Address Node ID for the User.

ATALK_NET
A number that represents the AppleTalk Address Network Number for the User.

ENABLE_CALLBACK
Indicates if the Callback feature is enabled or disabled for the User. A value of TRUE indicates that the Callback feature is enabled, while FALSE means it is disabled.

ENABLE_USER_AUTH
Indicates if User level Authentication is enabled or disabled for the User. A value of TRUE indicates that User level Authentication is enabled, while FALSE means it is disabled.

USER_AUTH_TIME
Indicates the last time that user level security authentication was preformed for the User.

AUTH_TIMEOUT
The grace period for User level Authentication, which is the amount of time, in minutes, that the user will not be re-authenticated at the user level.

USER_ACCUM

The SFVRA Service creates the entries in this table the first time a connection is established with a User. The table is updates on each connection thereafter. Clicking the Reset button in the Client interface clears the values for CUR_MIN_IN_DAY, CUR_MIN_IN_MONTH, CUR_MIN_OUT_DAY, and CUR_MIN_OUT_MONTH for the User.

USER_NAME
The user to which the in this table belongs.

CUR_MIN_IN_DAY
The number of minutes used for incoming calls from the user to the CyberSWITCH so far this day. Note that this number does not include any calls that are currently active.

CUR_MIN_IN_MONTH
The number of minutes used for incoming calls from the user to the CyberSWITCH so far this month. Note that this number does not include any calls that are currently active.

CUR_MIN_OUT_DAY
The number of minutes used for outgoing calls from the CyberSWITCH to the user so far this day. Note that this number does not include any calls that are currently active.

CUR_MIN_OUT_MONTH
The number of minutes used for outgoing calls from the CyberSWITCH to the user so far this month. Note that this number does not include any calls that are currently active.

CUR_BANDWIDTH
The bandwidth of current calls with the User.

CUR_DAY
An integer number that represents the day for which the table entry was last updated.

CUR_MONTH
An integer number that represents the month for which the table entry was last updated.

USER_CATEGORIES

Entries are created in the table by the Client interface as the administrator configures them. The SFVRA Service does not use this information.

CATEGORY_ID
A number that uniquely represents the CATEGORY_NAME, which is stored in the USER_ACCESS table.

CATEGORY_NAME
A string created by the administrators of SFVRA-CONN's Client interface to do their own categorizing.

USER_INFO

Entries are created in this table by the Client interface for every User configured.

Note: For every entry in the USER_INFO table there must be a corresponding entry in the USER_ACCESS table.

USER_NAME
A string used to uniquely identify a User.

NAME_LAST
Identifies a responsible person for the User. The SFVRA Service does not use this information.

NAME_FIRST
Identifies a responsible person for the User. The SFVRA Service does not use this information.

ADDR1
Identifies the address of a responsible person for the User. The SFVRA Service does not use this information.

ADDR2
Identifies the address of a responsible person for the User. The SFVRA Service does not use this information.

POST_CODE
Identifies the ZIP code of a responsible person for the User. The SFVRA Service does not use this information.

CITY
Identifies the city of a responsible person for the User. The SFVRA Service does not use this information.

STATE
Identifies the state of a responsible person for the User. The SFVRA Service does not use this information.

COUNTRY
Identifies the country of a responsible person for the User. The SFVRA Service does not use this information.

TELEPHONE1
Identifies a telephone number of a responsible person for the User. The SFVRA Service does not use this information.

TELEPHONE2
Identifies a telephone number of a responsible person for the User. The SFVRA Service does not use this information.

FAX
Identifies the fax number of a responsible person for the User. The SFVRA Service does not use this information.

EMAIL
Identifies the email address of a responsible person for the User. The SFVRA Service does not use this information.

ACCT_ID
The ACCT_ID is reserved for a future feature. The SFVRA Service does not use this information. ACCT_ID is not currently supported.

Note: ACCT_ID cannot be NULL, even though this field is not currently supported.

ACCT_STATUS
The ACCT_STATUS is reserved for a future feature. The SFVRA Service does not use this information. ACCT_STATUS is not currently supported.

CATEGORY_ID
Identifies the category stored in the USER_CATEGORIES table for the User. The SFVRA Service does not use this information.

ORGANIZATION
Identifies the organization of a responsible person for the User. The SFVRA Service does not use this information.

COMMENTS
Represents any comments that the administrator may need in relation to this User. The SFVRA Service does not use this information.

ACCT_START_DATE
The ACCT_START_DATE is reserved for a future feature. The SFVRA Service does not use this information. ACCT_START_DATE is not currently supported.

ACCT_END_DATE
The ACCT_END_DATE is reserved for a future feature. The SFVRA Service does not use this information. ACCT_END_DATE is not currently supported.

USER_RESERVED

Entries are created in this table by the Client interface when the administrator defines a User as reserved during CyberSWITCH configuration. The SFVRA Service uses this table to dole out reserved channels as defined in the ISDN_CHAN_RESERVED and MODEM_CHAN_RESERVED columns of the ACCESS_SERVER table.

SERVER_NAME
The CyberSWITCH on which the User defined by USER_NAME has reserved status.

USER_NAME
The Users that have reserved status on the CyberSWITCH defined by SERVER_NAME.

CONNECTTYPE_ID
The type of connection for the User as referenced in the USER_CONNECTTYPES table.

USER_AUTHENTICATIONS

This table is currently not in use by the current version of the SFVRA Service or the Client interface and will be removed at a later date. The inclusion of this table is necessary for backward compatibility.

AUTHENTICATION_ID
AUTHENTICATION_ID is not currently supported.

AUTHENTICATION_NAME
AUTHENTICATION_NAME is not currently supported.

USER_CONNECTTYPES

Entries are created in this table when the database is installed or upgraded.

CONNECTTYPE_ID
A unique number used to identify the type of connection to make to a User. Refer to the Connection Type options table below to translate the connection type codes.

CONNECTTYPE_NAME
A string representation of the ID type.

USER_LAYER2

This table is currently not in use by the current version of the SFVRA Service or the Client interface and will be removed at a later date. The inclusion of this table is necessary for backward compatibility.

LAYER2_ID
LAYER2_ID is not currently supported.

LAYER2_NAME
LAYER2_NAME is not currently supported.

USER_CALLDIRECTIONS

Entries are created in this table when the database is installed or upgraded.

CALLDIRECTION_ID
A unique number used to identify the direction of the call with a User.

CALLDIRECTION_NAME
A string representation of the ID.

CONN_REPORT_HDR

The Client Interface uses this table to create reports defined by the administrator. This table is filled with the information defined by the date range and type of report from the Reports dialog of the Client Interface when either the *Preview* or *Print* buttons are clicked. This table should not be modified.

CONN_REPORT_DET

The Client Interface uses this table to create reports defined by the administrator. This table is filled with the information defined by the date range and type of report from the Reports dialog of the Client Interface when either the *Preview* or *Print* buttons are clicked. This table should not be modified.

ROUTING_PROTOCOLS

Entries are created and updated by the Client interface.

PROTOCOL_ID
Indicates the version of RIP to use. Refer to the RIP options table below to translate the RIP codes.

Code	RIP Options
0	Version 1
1	Version 2

METRIC
METRIC is not currently supported.

CURRENT_TIME_EX

Entries are updated by the SFVRA Service and used by the Client interface to determine the current time on the machine on which the database resides.

TIME_NOW
Indicates the current time of the machine on which the database resides after a stored procedure is executed.

GROUPS

Entries are created in this table by the Client interface when a administrator creates a new Group.

GROUP_ID
A unique number identifying the GROUP_NAME. This number is also used in the ACCESS_SERVER and USER_ACCESS tables to assign groups to CyberSWITCH systems and Users. Group numbers are assigned according to the order that they are entered into the database. Note that a value of 1 is the No_Group.

GROUP_NAME
A string representation created by an administer for Groupings.

USER_GROUPS

Entries are created in this table when a User is added to more than one group. When a User belongs to more than one group, the GROUP_ID in the USER_ACCESS table is 0 and the group correlations for the User are found in this table. Users are listed once for each group to which they belong.

USER_NAME
The user for which this GROUP_ID is valid.

GROUP_ID
A number from the GROUPS table that indicates a group to which the User belongs.

SFVRA_SERVER

Entries are created in this table by the Client interface when an administrator configures SFVRA Services.

IP_ADDRESS
The IP Address of an SFVRA Service.

DESCRIPTION
A description of the SFVRA Service to aid the administrator. The SFVRA Service does not use this information.

RIP_SERVICE

Entries are created in this table by the Client interface when an administrator configures Network Proxy Services.

Note: Although the title of this table is RIP_SERVICE, it contains information for both the RIP Services and the Proxy ARP Services.

NAME
The name of an Windows NT machine on which an SFVRA Network Proxy Service is running.

GROUP_ID
A number indicating for which Group the Network Proxy Service will advertise routes.

DESCRIPTION
A description of the Network Proxy Service to aid the administrator. The SFVRA Service does not use this information.

VERSION

The entry in this table is created when the database is installed or upgraded. It indicates what version of the SFVRA database is being run to ensure that the Client interface and SFVRA Service do not attempt to reference fields that do not exist in the database.

VERNUMBER
The version number of the database. It is used by SFVRA to ensure the fields it is trying to reference are there.

ISSUE
The issue number of the database. It is used by SFVRA to ensure the fields it is trying to reference are there.

GETTING ASSISTANCE

REPORTING PROBLEMS

For a fast response, please take the time to fill out the System Problem Report to inform us of any difficulties you have with our products. A copy of this report can be found at the end of this chapter. This report provides us with important information to diagnose and respond to your questions. Please pay special attention to the following areas:

FAX Header
The System Problem Report has been designed as a FAX form. Please fill in all information in this area before you FAX the report to Cabletron Systems. If you plan to mail the System Problem Report, please fill in the company information in this section for reference information.

Software
Please fill in the following sections:
- SFVRA-CONN Client and Database Version (From the About box.)
- Central Site Release, Issue, and Version (From the VERsion command.)

Hardware
Select the Platform and resources that you are using.

Problem
Please fill in the following sections:
- Type (Software, Hardware, Unknown.)
- Occurrence (Reproducible, Intermittent, Single Occurrence.)
- Original Number (This field is for your use. Enter your problem tracking number, if desired, for future reference.)
- Description (Briefly describe the problem you are experiencing.)

Description (including sequence of events):
Briefly describe the problem you are experiencing. As best you can, describe the events or conditions that led to the problem you are experiencing.

Please send the System Problem Report form and any extra information (for example, line traces, system reports, and configuration files) that you have.

CONTACTING CABLETRON SYSTEMS

You can call us directly at:

Phone: (603) 332-9400
FAX: (603) 337-3075 fax

or, you can send email to us at:

support@ctron.com

DATE: _____ NUMBER OF PAGES INCLUDING THIS PAGE: _____

TO: CUSTOMER SERVICE
Cabletron Systems
(603) 332-9400 PHONE
(603) 337-3075 FAX

FROM: _____
COMPANY:_____
ADDRESS: _____
_____
PHONE: _____
FAX: _____

CABLETRON SYSTEMS
SYSTEM PROBLEM REPORT

SOFTWARE

SFVRA-CONN Client Version: _____ Database Version: _____

Central Site Release: _____ Issue: _____ Version: _____

PROBLEM

Type	Occurrence
__ Hardware	__ Reproducible
__ Software	__ Intermittent
__ Unknown	__ Single Occurrence

DESCRIPTION (including sequence of events prior to problem occurrence):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

CABLETRON SYSTEMS USE ONLY

Control No:	Priority:	Date Received:
Resolution:		

INDEX

A

ACCESS_SERVER 198
ACCESS_SERVER_STATUS 200
Adobe Acrobat Reader 28
AppleTalk 58
  example network 184
  network number 58
  node ID 59
  routing protocol 59
applications
  Convert 131
  CSX Monitor 139
  Manage Logins 129
  SQL Setup Utility 124
authentication
  CHAP 65
  CLID 67
  device level 63
  PAP 65
  user level 64
  Windows NT 66

B

backing up data 105
base data rate 61
baud rate 74
bearer capabilities 74
bridging 53
  dial out 53
  example networks 141
  IP RLAN 55
  IPX RLAN 56

C

call detail recording 14
CALL_HISTORY 203
callable
  AppleTalk 58
  bridging 54
  IP 43
  IPX 47
callback 70
CALLING_NUMBERS 200
channels 35
CHAP
  secret 66
  security 65
CLID 67
  user entry 74
compression control protocol 70
CONN_REPORT_DET 218
CONN_REPORT_HDR 218
CONNECT _HISTORY 204
connections
  current 89
  history 92
  problem log 96
  reports 100
  status 91
Convert 131
CSX configuration file conversion 134
CSX Monitor 139
current
  connections 89
CURRENT_CALL 205
CURRENT_CONNECT 206
CURRENT_TIME_EX 218
CyberSWITCH
  group 35
  name 34
  pooling 37
  priority users 36
  properties 34

D

data
  backing up 105
data file conversion 135
database
  access 130
  information 103
  installation 25, 124
  upgrade 107, 127
dbmssocn.dll 23
destination subnet 45
detailed user reports 101
device level authentication 18, 63

dial out
connect type 73
number 73
subaddress 74
dynamic address assignment 18, 44

E
error messages
Client 112
Convert 136
ethernet address 67
example networks
AppleTalk 184
bridging 141
IP 152
IPX 169
export
connect history 93
problem log 98
reports 102

F
failure messages 121
FAILURE_TYPES 202
feature overviews
bandwidth agility 14
call back 14
call restriction 14
centralized management 14
high availability 15
load leveling 15
network security 15
pooling 15
protocol discrimination 15
user discrimination 15
file conversion
CSX configuration files 132
data files 134

G
GROUPS 218
groups
assignment verification 110
CyberSWITCH 35, 79
overview 78
RIP or Proxy ARP Service 87
user 68, 80
view 81

H
H0 call support 62
help
contacting Cabletron Systems 221
history
connections 92
hunt groups 18

I
informational messages
Client 117
Convert 138
initial bandwidth 61
installation
Adobe Acrobat Reader 28
database 25, 124
different location 125
MS SQL Server 21
NDIS driver 26
ODBC driver 21
SNMP service 27
software 24
interrogative messages
Client 118
Convert 138
IP 43
address pools 14, 37
dynamic address assignment 44
example network 152
filters 44
IP address
CyberSWITCH 34
SFVRA service 85
user 43
IP_POOL 201
IPX 46
example network 169
IPX WAN protocol 47
packet handling features 52
routing protocol 48
spoofing features 51
SPX protocol 50
WAN peer type 48
Watchdog protocol 49

L
LMHOSTS 23
load leveling 70
login ID 129
requirements 29, 124, 130, 134, 140

M

Manage Logins 129
manage tables
  connect history 93
  problem log 98
maximum bandwidth 61
message packet handling 52
messages
  Client
    error 112
    failure 121
    informational 117
    interrogative 118
    reasons for failure 122
    warning 117
  Convert
    error 136
    informational 138
    interrogative 138
    warning 137
  SQL error 121
metric value 45
MIB file
  compiling 27
  location 27

N

NDIS driver
  installation 26
network number
  AppleTalk 58
  IP RLAN 54
  IPX RLAN 54
network proxies 86
  properties 83
  SFVRA services 84
NT security 66

O

ODBC driver
  installation 21
on-node device database 40

P

PAP
  password 66
  security 65
passwords 129
PPP STAC-LZS number 71
problem log 96
problem report 101
  system 222
PROBLEM_LIST 202
protocols
  Users 42
proxy ARP service 86
  operation 31
  starting/stopping 32

R

REASON_STRINGS 202
release notes 12
Remote Access Switch
  pooling 37
  priority users 36
  properties 34
remote devices 16
remote LAN
  IP 55
  IPX 56
    network number 54
reporting problems 221
reports 100
  creating 102
  detailed 101
  problem 101
  summary user 100
restrictions 60
  configurable features 62
  current usage 76
  reset 76
RIP 18
  properties 83
  service 31
RIP service 86
  starting/stopping 32
RIP_SERVICE 219
routing protocol 84
ROUTING_PROTOCOLS 218
RTMP 59

S

search
  current
    connections 90
  history
    connect 92
  problem log 96
security
  authentication process 63
serialization packet handling 52

services
proxy ARP 31
RIP 31
SFVRA 30
starting / stopping 32
SFVRA
enabled on CSX
operation verification 109
service 30, 84
SFVRA Connection Manager
functions 13
SFVRA_SERVER 219
SNMP
compiling MIB file 27
configuring service 27
installing service 27
software
installation 24
upgrade 105
spoofing options 51
SPX protocol 50
SQL error messages 121
SQL Server
installation 21
SQL server
setup utility 124
STAC-LZS number 70
static routes 13, 45
STATIC_IP_ROUTES 201
subaddress 74
subnet mask 45
summary user report 100
system messages
reasons for failure 122
System Problem Report 222
system requirements
client 18
server 17

T
TCP connections
monitor 139
operation verification 108
problem diagnosis 111
TCP port number 34
telephone number 73
tempdb
expanding 126
troubleshooting 108, 111

U
unnumbered interfaces 18, 43
upgrade
database 107, 127
software 105
user level authentication 64
grace period 68
USER_ACCESS 207
USER_ACCUM 214
USER_AUTHENTICATIONS 217
USER_CALLDIRECTIONS 217
USER_CATEGORIES 214
USER_CONNECTTYPES 217
USER_GROUPS 219
USER_INFO 215
USER_LAYER2 217
USER_RESERVED 216
Users
access 63
address and contacts 41
category 42
contacts 41
list 40
name 41
protocols 42
AppleTalk 58
bridging 53
IP 43
IPX 46
restrictions 60
telephone 72
usage 76

V
verifying
group assignments 110
TCP connection 108
VERSION 220

W
warning messages
Client 117
Convert 137
watchdog protocol 49
Windows NT
authentication 66
WINS 23